Title: Function Risk Assessment for <System Name>		Page 1 of 9
Document No.:	<Document No.>	

Functional Risk Assessment for <System Name>

[Appendix 2i-Template of Functional Risk Assessment]

Pre-APPROVAL PAGE

Prepared By:

Name	Designation	Department	Signature	Date

Reviewed By:

Name	Designation	Department	Signature	Date

Approved By:

Name	Designation	Department	Signature	Date

[Appendix 2i-Template of Functional Risk Assessment]

TABLE OF CONTENTS

REVISION HISTORY

Revision No	Effective Date	Reason of Change
		Initial Document

[Appendix 2i-Template of Functional Risk Assessment]

1.0 PURPOSE:

2.0 SCOPE:

3.0 REFERENCES:

4.0 RESPONSIBILITIES:

5.0 RISK COUNT:

5.1 RISK ASSESSMENT:

Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards (as defined below). Risk assessments begin with a well-defined problem description or risk scenario. When the risk in question is well defined, and the types of information that will address the risk scenario will be more readily identifiable. As an aid to clearly defining the risk (s) for risk assessment purposes, three fundamental questions are often helpful:

1. What might go wrong?
2. What is the likelihood (probability) it will go wrong?
3. What are the consequences (severity)?

The overall process follows Failure Modes and Effects Analysis (FMEA) model. FMEA identifies the opportunities for failure, or "failure modes," in each step of the process.

5.1.1 IDENTIFYING RISK SCENARIOS:

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

The functions identified are analyzed by considering possible hazards and what controls may be needed to minimize the potential harm.

Following types of risks are mainly considered during risk assessment process for use of computerized systems in regulatory environment but, are not limited to these ones only:

- Risks due to non-availability of System Access Control and Authorizations
- Risks due to abnormal user operation performed at the time of system operation
- Risk due to non-availability of SOP/WI

Each failure mode gets a numeric score that quantifies

(a) likelihood or probability that the failure shall occur (P)

(b) the amount of harm or damage the failure mode may cause (S)

(c) likelihood that the failure shall not be detected (D).

The product of these three scores is the Risk Priority Number (RPN) for that failure mode.

5.1.2 ASSESSING THE LIKELIHOOD OR PROBABILITY:

After identifying risk scenario, determine the likelihood or probability of it occurring. User considers the probability of the hazard occurring per number of transactions/duration, and assigns a value to that estimate.

RANKING OF PROBABILITY IS DEFINED AS FOLLOWS:

Value	(P) Probability of Failure (Likelihood of occurrence)
3	High(H): Often
2	Medium(M): Periodic
1	Low(L): Seldom

5.1.3 ASSESSING THE SEVERITY OF IMPACT:

The amount of harm or damage the impact of the risk scenario may cause is assessed. Impact on regulatory compliance, impact on product quality and impact on data integrity are considered when evaluating severity.

RANKING OF SEVERITY:

Value	(S) Severity of impact (Consequence)
1	Low(L): No Impact on Product Quality No Impact on Overall System Performance and/or Functionality No Impact on Operator Safety. No exception or gap with respect to regulations or standards (GxP, EU, GAMP, ASTM, etc.) Insignificant impact on data security/integrity/GxP requirements.
2	Medium(M): Minor Impact on Product Quality Minor Impact on Overall System Performance and/or Functionality Minor Impact on Operator Safety Indirect and significant impact on data security/integrity/GxP requirements.
3	High(H): Major Impact on Product Quality Major Impact on Overall System Performance and/or Functionality Major Impact on Operator Safety Exception or gap with respect to regulations or standards (GxP, EU, GAMP, ASTM, etc.) Direct and significant impact on data security/integrity/GxP requirements.

5.1.4 DETECTION:

Identify if the risk scenario can be recognized or detected. Risk scenarios and their impacts having high probability of detection, may not pose a serious threat because it can be recognized quickly and suitable corrective action can be taken to mitigate them. If there is a low probability of detection, then the risk scenario needs to seriously consider a review of the design or the implementation of alternative procedures to avoid them.

RANKING OF DETECTION:

Value	(D) Level of Detection
1	High (H): The risk scenario can be easily detected through deployed control measure/system and the detection system is automated. e.g. 100% detection or inspection technique is in place specifically for the failure like an alarm, interlock, error message or system shutdown.
2	Medium (M): The risk can be detected later through deployed control measure/system and the detection is through manual method. e.g. Detected by indirect means or by observation like indirect indication or visual inspection.
3	Low (L): The risk cannot be detected through deployed control measure/system and the detection is possible after a long period/interval.

5.1.5 RISK PRIORITY NUMBER

The Risk Priority Number, or RPN, is a numeric assessment of risk scenario as part of Failure Modes and Effects Analysis (FMEA), in which team assigns each failure mode numeric values that quantify likelihood of occurrence, likelihood of detection, and severity of impact. The final risk priority is calculated based on following equation.

RPN = Probability x Severity x Detection

The table below depicts RPN numbers considered for classifying overall priorities

Overall priority	RPN	Measures
Low	1 to 5	Acceptable. No additional measures required.
Medium	6 to 9	Additional measures required to mitigate the risk. Additional measures may be procedural or technical.
High	10 to 27	Additional measures required to mitigate the risk. Additional measures may be procedural or technical. May require design change to address risk scenario.

5.1.6 RISK MITIGATION AND CONTROL:

Low risk scenarios shall require only good IT/QA/QC/Engineering practices. Medium risk scenarios shall require additional measures and controls. High risk scenarios shall require additional measure and controls. High risk scenarios may require design changes.

Measure and controls shall be traceable to identified risks and shall be verified during qualification to ensure that they are effective in producing the intended risk reduction. The reference document section is used to document the test protocols, SOP and other documents for traceability.

Following is the verification strategy based on the risk priority

- For low risk, verification of configuration SOP shall be done.
- For medium risk, in addition to verification of the configuration, functionality impacted by the configuration shall be verified.
- For high risk, in addition to verification of the configuration, relevant risk scenarios impacted by the configuration shall be verified.

For medium and high-risk scenarios after the implementation of measures to reduce the risk, the RPN is reevaluated and recalculated as outlined in section. The aim is to reduce the risk priority to Low

6.0 Risk Assessment Report:

For the Functional Risk Assessment of [NAME OF SYSTEM] as defined in the scope following risk scenarios, impact, and measures were considered. Prioritized the fault conditions associated with each adverse event based upon those areas of greatest susceptibility. The risk priority of the fault conditions is used to select the appropriate risk measure.

7.0 FUNCTIONAL RISK ASSESSMENT DOCUMENTATION TABLE:

Sr. No.	Risk Scenario	Impact	P	S	D	RPN/Risk level	Risk Acceptance (Yes/No)	Current Controls	Recommended Measures/Mitigation	Residual Risk				Risk Acceptance (Yes/No)	Measures Taken/Related Qualification Tests	Complied By
										P	S	D	RPN/Risk level			
1.																

8.0 Conclusion

9.0 Abbreviation

[Appendix 2i-Template of Functional Risk Assessment]

POST-APPROVAL PAGE

Prepared By:

Name	Designation	Department	Signature	Date

Reviewed By:

Name	Designation	Department	Signature	Date

Approved By:

Name	Designation	Department	Signature	Date