COMPUTER SYSTEM RISK EVALUATION FOR DETERMINING RISK MITIGATIONS, VALIDATION ACTIVITIES, AND THE EXTENT OF TESTING

1. PURPOSE

This procedure provides a method for managing the risks associated with computer system failure. It includes the identification of hazards and potential failures associated with an item, the evaluation of associated risks, and taking action to reduce those risks.

2. SCOPE

This risk management procedure can be used for formal risk management efforts in conjunction with computer systems, including custom developed software and purchased systems.

3. REFERENCE DOCUMENTS

[Note to the purchaser of this document: Many of the policy documents, procedures, and templates referenced here are available at www.BPAconsultants.com or www.ComplianceOnline.com]

3.1. RISK001 – Risk Management Policy

3.2. ISO14971:2000, Medical devices – Application of Risk Management to Medical Devices

3.3. VAL003 – Validation of Computer Systems Used in Production and Quality Systems

3.4. VAL003 – Life Cycle for the Selection, Implementation, Validation and Use of Computer Systems

3.5. VAL019 - Guidance on Validation Activities for Systems at the Low-, Moderate, and High-Risk Levels

3.6. Stein, R. Timothy. *The Computer System Risk Management and Validation Life Cycle,* Paton Press, 2006

4. DEFINITIONS

4.1. ALARP: As Low As Reasonably Practicable

4.2. Area: Aspects of the item that involve potential failures/hazards. An area may be a module, component, or subcomponent of the item.

4.3. Business harm: The impact the failure/hazard will have on item or company's efficiency.

4.4. Clinical harm: The impact the failure/hazard will have on the quality of the product or safety of the patient.

COMPUTER SYSTEM RISK EVALUATION FOR DETERMINING RISK MITIGATIONS, VALIDATION ACTIVITIES, AND THE EXTENT OF TESTING

4.5. Compliance harm: The impact of the failure/hazard on compliance with the company's policy, and/or external standards and regulations.

4.6. Economic practicality: The ability to reduce risk without making the product/item an unsound economic proposition.

4.7. Failure: Performance of an item in a way that is not consistent with the manner in which it was intended to function.

4.8. Harm: Physical injury to the health of people, damage to property or the environment, or damage to the company's ability to comply with appropriate regulations.

4.9. Hazard: Potential source of harm. The term "hazard" connotes potential physical harm as the result of an item failure, misuse or breakdown.

4.10. Item: Any item that is the subject of risk management. Examples of such items include products, systems, equipment, processes, and computer systems.

4.11. Item Owner: The manager of the department, or designee, that is most impacted by, or is the primary user of, the item.

4.12. Residual risk: Risk remaining after protective measures have been taken.

4.13. Risk: Combination of the probability of occurrence of harm and the severity of that harm.

4.14. Risk analysis: Systematic use of available information to identify failures or hazards and to estimate the risk of such failures or hazards.

4.15. Risk assessment: A process compromised of risk analysis and risk evaluation.

4.16. Risk control: The process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.

4.17. Risk evaluation: Judgment, on the basis of risk analysis, of whether a risk that is acceptable has been achieved in a given context based on the current values of society.

4.18. Risk management: Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating and controlling risk.

4.19. Risk management file: Set of records and other documents, not necessarily contiguous, that are produced by a risk management process.

4.20. RiskVal Life Cycle: The life cycle for computer system risk management and validation in *The Computer System Risk Management and Validation Life Cycle.*

4.21. Severity: Measure of the possible consequences of a hazard.

COMPUTER SYSTEM RISK EVALUATION FOR DETERMINING RISK MITIGATIONS, VALIDATION ACTIVITIES, AND THE EXTENT OF TESTING

7. QUALITY RECORDS

Record Name	Record Format	Record Owner	Storage Location	Filing Method
Risk Management File (if a file is kept that is separate from the validation report)	Unspecified. Includes all components identified in this procedure	QA	QA	By system name
The following are kept as the Risk Management File or as part of the Validation Record				
High Level Risk Assessment Report (if a separate report is created)	See 6.3.14.3	QA	QA	With the Risk Management Report or Validation Report for the System
Detailed Risk Assessment Report	See 6.3.14.3	QA	QA	With the Risk Management Report or Validation Report for the System
Mitigation Plan (if any)	Unspecified	QA	QA	With the Risk Management Report or Validation Report for the System
Mitigation Report (if any)	Unspecified	QA	QA	With the Risk Management Report or Validation Report for the System

(Note that the Record Owner is the function that keeps the records, and not the function that creates the record).

8. SUMMARY OF REVISION CHANGES AND JUSTIFICATION

8.1. The changes created in this revision, and their justifications are provided in the following table.

Changes	Justification
1. New document	A procedure is provided for the management of risk.