|  |
| --- |
| This SOP Template (template) is being provided by Praxis Management International, LLC (Praxis) for the "fair use" by you, the User, as that term is defined under the U.S. Copyright Laws. All other use, reproduction or re-transmission in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, without prior written permission from Praxis is prohibited. ©2008-2015 Praxis Management International, LLC. All rights reserved.Praxis makes no representations or warranties concerning the suitability or use of, or reliance on, the Template. Any actual or implied representation or warranty that the Template does not infringe the intellectual property rights of any third party is specifically hereby void. Any special, indirect or consequential damages or any damages whatsoever resulting from the use or misuse of the Template, the loss of use, data, or profits, whether in an action of contract, negligence, or other tortious action arising out of or in connection with the Template shall be born exclusively by the User. |

**Contents**

[SOP Purpose 3](#_Toc429134051)

[SOP Scope 3](#_Toc429134052)

[Definitions 3](#_Toc429134053)

[Responsibilities 3](#_Toc429134054)

[Risk Management Overview 3](#_Toc429134055)

[Risk Management Process 4](#_Toc429134056)

[Risk Assessment 4](#_Toc429134057)

[Risk Control 4](#_Toc429134058)

# SOP Purpose

The purpose of this document is to provide a systematic approach to system quality risk management. This SOP defines the overall program of procedures and controls for managing system quality risks for the Information Technology systems used in regulated activities.

# SOP Scope

This SOP applies to all computer-based systems.

# Definitions

Hazard: A potential source of harm

Risk: A measure of the severity and probability of a hazard

Risk Assessment: A comprehensive evaluation of risks and associated impacts

Criticality Level: a measure of the level of risk associated with a system or major system function

Risk Control: Actions taken to reduce the impacts of risks

Risk Management: A systematic approach to assessment and control of risks throughout the system life cycle

# Responsibilities

The Quality Manager is responsible for

* Leading risk assessments.
* Contributing expertise on compliance with regulations and regulatory guidelines.

The IT Manager is responsible for

* Implementing the practices for system risk management as specified within this SOP.
* Contributing technical expertise to each computerized system’s risk assessment
* Leading risk control activities for each computerized system

The Business Managers are responsible for

* Contributing business area expertise to each computerized system’s risk assessment.

# Risk Management Overview

The use of computerized systems in regulated activities imposes a degree of risk to both the regulated product and associated records. It is important to understand that software risk should be managed throughout the system’s life cycle. An effective quality risk management approach can ensure the quality of the system during both the development and production stages, as well as provide a framework for decision making should a quality issue arise.

# Risk Management Process

**RISK MANAGEMENT PROCESS**

**RISK IDENTIFICATION & ASSESSMENT**

**RISK CONTROL**

SOP

System

Risk Assessment

SOP

Risk Based Validation

SOP

Audit Trails

SOP

System Security

SOP

User Training

SOP

System Backup

SOP

Alternate Records

SOP

Software Vendor Assessment

SOP

Incident Management

## Risk Assessment

Risk assessment consists of the identification of hazards and the analysis of the risks associated with each hazard. In software, each area of system functionality could potentially fail to function as intended and is therefore a hazard.

Three fundamental questions are answered by software risk assessment:

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

For detail on conducting and documenting software risk assessments, see *SOP Risk Assessment.*

## Risk Control

Risk assessment consists of the decisions made to mitigate the probability and severity of harm. The amount of effort applied to risk control should be proportional to the significance of the risk.

Two questions are the focus of software risk control:

1. What can be done to reduce or eliminate risk?
2. What is the appropriate balance among benefits, risks, and resources?
	1. Which risks should be reduced?
	2. Which risks should be accepted?

Risk reduction mechanisms are applied throughout the system life cycle. Here are some examples:

| **Risk Reduction Mechanisms** |
| --- |
| **Procedure** | **Controls determined by system and feature criticality** |
| *SOP Risk Based Validation* | * Scope and extent of initial validation and validation of system changes, including
	+ Documentation requirements
	+ Testing coverage
 |
| *SOP Audit Trails* | * Need for audit trails
* Audit trail features
* Audit trail validation requirements
 |
| *SOP System Security* | * System back-up audit schedule
* Password change schedule
 |
| *SOP Software Vendor Assessment* | * Vendor assessment method
 |
| *SOP User Training* | * Training method and format
* Re-training requirements for system changes
* Training effectiveness review schedule
 |
| *SOP Incident Management* | * Incident investigation and resolution priority
* Requirement for users notification of incidents and workarounds
 |
| *SOP System Backup* | * Back-up schedule
* Back-up storage location
 |
| *SOP Alternate Records* | * Verification of data entry
 |

Risk acceptance is the decision to accept risk. Even after risk reduction mechanisms are applied via the procedures, above, some risk remains. This residual risk can either be accepted or further reduced.

For example, SOP Alternate Records does not require second person verification of data entry for systems with a criticality level of “Medium”. Therefore, business managers of medium criticality systems can decide to either:

* accept the residual risk of not having second person data entry verification
* apply the risk reduction mechanism of second person data entry verification.

**References:**

*Eudralex Volume 4, Annex 15: Qualification and Validation*, European Commission, July 2001

*General Principles of Software Validation; Final Guidance for Industry and FDA Staff*, FDA, January 11, 2002

*Glossary of Computerized System and Software Development Terminology*, FDA, April 30, 2003

*Good Practices for Computerised Systems in Regulated “GxP” Environments*, PIC/S, September, 2007

*Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices*, FDA, September 9, 1999

*Guidance for Industry: Computerized Systems Used in Clinical Investigations*, FDA, May, 2007

*Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application*, FDA, August 2003

*Guidance for Industry: Q9 Quality Risk Management*, FDA, June, 2006

 *21 CFR Part 820, Quality System Regulation*, FDA, April 1, 2007