RISK ANALYSIS

Project or System Name

U.S. Department of Housing and Urban Development

Month, Year

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	1/31/00	SEO&PMD Risk Analysis
Rev. 1	5/1/00	Risk Analysis Template and Checklist
Rev. 2	6/14/00	Minor changes per Office of Administration
Rev. 3	4/12/02	Conversion to WORD 2000 Format

Risk Analysis Authorization Memorandum

I have carefully assessed the Risk Analysis for the (System Name). This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____	_____
NAME Project Leader	DATE
_____	_____
NAME Operations Division Director	DATE
_____	_____
NAME Program Area/Sponsor Representative	DATE
_____	_____
NAME Program Area/Sponsor Director	DATE

RISK ANALYSIS

TABLE OF CONTENTS

Page #

1.0 GENERAL INFORMATION

NOTE TO AUTHOR: *Highlighted, italicized text throughout this template is provided solely as background information to assist you in creating this document. Please delete all such text, as well as the instructions in each section, prior to submitting this document.* ***ONLY YOUR PROJECT-SPECIFIC INFORMATION SHOULD APPEAR IN THE FINAL VERSION OF THIS DOCUMENT****.*

The determination of the type of risk assessment to be performed relates to the decision made during the category determination process described in section 1.3 of the System Development Methodology. The level of effort required to perform a risk analysis will be much greater for a new development effort than for an enhancement of a system.

1.0 GENERAL INFORMATION

1.1 Purpose

Describe the purpose of the Risk Analysis.

1.2 Scope

Describe the scope of the Risk Analysis as it relates to the project.

1.3 System Overview

Provide a brief system overview description as a point of reference for the remainder of the document. In addition, include the following:

- Responsible organization
- System name or title
- System code
- System category
  - *Major application*: performs clearly defined functions for which there is a readily identifiable security consideration and need
  - *General support system*: provides general ADP or network support for a variety of users and applications
- Operational status
  - Operational
  - Under development
  - Undergoing a major modification
- System environment and special conditions

1.4 Project References

Provide a list of the references that were used in preparation of this document. *Examples of references are:*

- *Previously developed documents relating to the project*
- *Documentation concerning related projects*
- *HUD standard procedures documents*

1.5 Acronyms and Abbreviations

Provide a list of the acronyms and abbreviations used in this document and the meaning of each.

1.6 Points of Contact

1.6.1 Information

Provide a list of the points of organizational contact (POC) who may be needed by the document user for informational and troubleshooting purposes. Include type of contact, contact name, department, telephone number, and e-mail address (if applicable). Points of contact may include, but are not limited to, helpdesk POC, development/maintenance POC, and operations POC.

1.6.2 Coordination

Provide a list of organizations that require coordination between the project and its specific support function (e.g., installation coordination, security, etc.). Include a schedule for coordination activities.

2.0 PROJECT AND SYSTEM DESCRIPTION

2.0 PROJECT AND SYSTEM DESCRIPTION

This Risk Analysis document provides an approach for conducting risk assessments of implemented systems, systems under development, microcomputer systems, implemented applications, and applications under development. The approach is adaptable for conducting the different types of risk assessments, whether it is for a personal computer (PC), large system or application, or whether it is for a system or application that is implemented or under development. It allows an informal review or short-form risk assessment to be conducted when it is determined that the system or application being assessed is, or will be, a microcomputer-based system.

2.1 Summary

Provide basic information about the project and the application system for which a risk analysis is being conducted.

2.1.1 Project Management Structure

Identify the project sponsor, sponsoring office project leader, and the estimated or actual start and end dates of a new or modified system project.

2.1.2 Project Staffing

Determine the approximate number of staff hours required (HUD personnel and contractors) and identify the expertise, knowledge, skills, and abilities needed by the project team to develop and/or maintain a quality application system. Staff hours should be broken down by major skill category, both technical and program related. This information will help management determine the resources required and when they are needed.

2.2 Risk Management Structure

Identify organizations responsible for managing identified risks and maintaining countermeasures.

2.3 Periodic Risk Assessment

Describe the frequency of periodic risk assessments of the operational system.

2.4 Contingency Planning

Determine the level of contingency planning needed and identify the responsible personnel involved.

3.0 SYSTEM SECURITY

3.0 SYSTEM SECURITY

Based on the environment, scope, sensitivity of the data, and criticality of the proposed system to the project sponsor and users, assess the security requirements and specifications necessary to safeguard the system and its corresponding data. Include such information as privacy requirements, estimated dollar value of assets, and contingency planning requirements (including the Business Resumption Plan).

3.1 Baseline Security Requirements

Analyze the processes and procedures required of the new system or the system to be replaced and the sensitivity of the data the system will be processing to determine inherent security risks. Determine the security controls that will be required to adequately counteract these security risks.

3.2 Baseline Security Safeguards

Describe the security-related technology that is currently available or projected to be available at the time the system is scheduled for operation. Determine potential safeguards against all identified risks and vulnerabilities, including those safeguards that may already be in place at HUD.

3.3 Sensitivity Level of Data

Evaluate the data being processed to determine whether the level of sensitivity requires safeguards, such as the application of security controls. In this evaluation, include input and output data, internally processed data, and data transmitted to or from the system.

3.4 User Security Investigation Level and Access Need

Analyze the system's end users, including those having direct access to the system and those who will indirectly receive output from the system. Determine the levels of security investigation and system access required for each user.

4.0 RISKS AND SAFEGUARDS

4.0 RISKS AND SAFEGUARDS

This section provides a detailed description of security risks and safeguards. Each risk should be under a separate section header, 4.1 - 4.x.

Evaluate the proposed system and its operational environment for potential risks and safeguards. For physical risks, determine the vulnerability of the computer room and the impact of environmental hazards on the computer, related equipment, and their contents. For communication risks, evaluate the system for threats to the privacy and authenticity of telecommunications. For hardware, review the system's current or proposed hardware configuration. For software, review the system software for security risks and potential vulnerabilities. Identify the potential security risks and provide the following information for each:

4.x [Risk Name]

Provide a risk name and identifier here for reference in the remainder of the subsection.

4.x.1 Risk Category

Identify the category of risk (physical, communications, hardware, software).

4.x.2 Risk Impact

Provide an assessment of the magnitude of the risk's impact in the event of an occurrence.

4.x.3 Potential Safeguard(s)

This subsection provides a detailed description of potential safeguards corresponding to the risk named in 4.x. Each safeguard should be under a separate subsection header, 4.x.3.1 - 4.x.3.y.

4.x.3.y [Safeguard Name]

Provide a name and identifier here for the potential safeguard for reference in the corresponding subsection of 5.x. Describe the safeguard.

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

Analyze the identified security threats and potential vulnerabilities of the proposed system, and determine the necessary measures to be taken to safeguard this system. Evaluate the identified measures for appropriateness and cost efficiency, and formulate a recommendation identifying those measures deemed suitable for implementation.

Each safeguard referenced in the corresponding section of 4.x.3.y should be under a separate section header, 5.1 - 5.x.

5.x Potential Safeguards

Review each of the safeguards identified in the corresponding subsection of 4.x.3.y and determine whether it is appropriate for use within the system's operational environment. Indicate its level of compatibility with the guidelines for operating information systems at HUD.

5.x.1 Lifecycle Costs for Acceptable Safeguards

Estimate the cost to develop, install, and operate each of the proposed system safeguards. Include user training and maintenance, if required, in these estimates.

5.x.2 Effect of Safeguards on Risks

For each of the proposed system's identified risks and vulnerabilities, estimate the extent to which the recommended safeguard will be effective in preventing or minimizing that threat or vulnerability.

5.x.3 Economic Feasibility of Safeguards

Contrast the lifecycle costs of each of the potential safeguards against the financial impact of the security risks they are designed to prevent. Consider the effect each safeguard is projected to have on minimizing those security risks. Determine whether the benefits achieved by these safeguards outweigh their operational and developmental costs.

6.0 RISK REDUCTION RECOMMENDATIONS

6.0 RISK REDUCTION RECOMMENDATIONS

Outline the potential security risks to the system to be developed or replaced and provide a detailed description of the security safeguards that are being recommended to counteract those risks.