DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

RISK ASSESSMENT TEMPLATE
Version 1.0

April 2005

FINAL

[SYSTEM NAME]
[Organization]

[DATE PREPARED]

Prepared by:

Preparing Organization

TABLE OF CONTENTS

SYSTEM NAME RISK ASSESSMENT REVIEW/APPROVAL SHEET

System Owner:		
Name:	**Signature**	**Date**

Security Officer:		
Name:	**Signature**	**Date**

Security Reviewer:		
Name:	**Signature**	**Date**

SYSTEM NAME RISK ASSESSMENT REVIEW SHEET

This Risk Assessment has been updated and approved on the following dates to account for the latest changes. This task will be completed at least annually.

Approval Date	Name of Security Officer	Signature of Security Officer

SYSTEM NAME RISK ASSESSMENT CHANGE INFORMATION PAGE

Issue	Date	Pages Affected	Description
Original	Date	All	Initial Draft Version

1.0 Introduction

A Risk Assessment is an important tool for Information Technology (IT) managers to use in evaluating the security of the IT systems that they manage, and in determining the potential for loss or harm to organizational operations, mission, and stakeholders. The risk assessment provides management with the capability to:

- Provide an adequate level of security protection for IT applications and systems.
- Meet Federal requirements for information and system security.
- Satisfy oversight organizations.
- Establish an acceptable level of risk.

Risk can never be totally eliminated, but can be minimized by the application of IT security controls. The decision as to what level risk will be accepted will be based on management review of the identified IT security controls needed to mitigate risk versus the potential impact of implementing those controls on available resources and system operations. The Risk Assessment identifies the current level of risk for the application and provides risk mitigation recommendations for management review. The Risk Assessment serves as the primary access control function for numerous critical applications and the loss of system availability and/or integrity that could have a debilitating impact on the organization's mission. The sensitivity level of the system and of the information stored within, processed by, or transmitted by the system reflects the value of the system to the organization. The sensitivity level has been used as the basis for implementing the necessary IT security controls for the system.

This risk assessment describes System Name vulnerabilities and associated threats based on executive, legislative, departmental, and technical guidelines. The Department of Housing and Urban Development Handbook 2400.25, the HUD ADP Security Program, establishes the policy, as well as organizational and management responsibility to implement the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; and Presidential Decision Directive 63 (PDD 63). The security risk assessment methodology is adapted from National Institute of Standards and Technology (NIST) *Risk Management Guide for Information Technology Systems*, Special Publication 800-30.

1.1. Purpose

The purpose of this report is to provide Operating Administration management with an assessment of the adequacy of the management, operational and technical security controls that are currently in place to secure System Name. This risk assessment report identifies threats and vulnerabilities applicable to System Name. It also evaluates the likelihood that vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identifies the overall risk level. This report documents risk assessment activities conducted by Risk Assessment Team Name personnel from Start Date to End Date, and will help Operating Administration management understand risks to System Name resources.

1.2. Scope

The scope of this risk assessment is to evaluate risks to System Name in the areas of management, operational, and technical controls. This risk assessment is limited to System Boundary and included site

visits to conduct interviews at Location of Interviews and physical security reviews of Locations Where Reviews Took Place.

Scope Exclusions:
[**Example**]: Excluded from this assessment are the mainframe platform (which is the general support system on which the system resides), the General Support System (located in the lower level of the Headquarters building), and the backbone network, all of which will be described within their respective certifications

1.3. Testing Methods

Vulnerabilities can be calculated through various tools, or testing methods, including the NIST *Recommended Security Controls for Federal Information Systems*, SP 800-53, vulnerability scans, results from the Security Testing and Evaluation Plan, and through various checklists that are specific to the software, hardware, or operating system with which System Name is configured. The following tools were used in calculating risk for System Name:

- insert tool name
- insert tool name

EXAMPLES OF TOOLS TO IDENTIFY HARDWARE, SOFTWARE AND OPERATING SYSTEM SECURITY REQUIREMENTS AND CONTROLS:

- NIST, Guidelines on Electronic Mail Security, SP-800-45, September 2002.
- NIST, Guidelines on Securing Public Web Servers, SP 800-44, September 2002.
- NIST Guidelines on Active Content and Mobile Code, SP 800-28, October 2001.
- NIST, Guidelines on Firewalls and Firewall Policy, SP 800-41, January 2002.
- NIST, DRAFT System Administration Guidance for Windows 2000 Professional, SP 800-43, January 28, 2002.
- National Security Agency (NSA), Windows 2000 Guides.
- NSA, Windows NT Guides.
- NSA, Cisco Router Guides.
- NSA, E-mail and Executable Content Guides

1.4. Document Structure

This document is organized into five sections:

- Section 1.0 provides the introduction, purpose, and scope of this risk assessment.
- Section 2.0 provides an overview of the risk assessment methodology.
- Section 3.0 provides a system description to include the system's information sensitivity and mission criticality.
- Section 4.0 provides the methodology to calculate risk, which includes identifying threats, likelihood, and impact.
- Section 5.0 provides the risk assessment results.

2.0 Risk Assessment Methodology

Risk analysis methodology is structured as four distinct phases:

- Risk analysis of resources, controls, threats, and vulnerabilities.
- Management decisions to implement security countermeasures and to accept residual risk.
- Implementation of countermeasures.
- Periodic review of the risk management program.

This document addresses the first phase, which provides the foundation for the remaining three phases. The detailed analysis of threat, vulnerabilities, and risks includes:

- **Asset Identification**: System resources within the system boundary that require protection.

- **Threat Sources and Vulnerability Identification**: Weaknesses in the system design, system security procedures, implementation, and internal controls that could be exploited by authorized operators or intruders.

- **Threat Identification**: Known and projected threats that are applicable to the system under review.

Prior to a risk assessment, security requirements must be identified. Security requirements are determined based on executive, legislative, and technical guidance in addition to departmental policy. Additionally, security requirements specific to the hardware, software, or operating system are also identified. The risk assessment is performed to identify the management, operational, and technical controls, or other appropriate countermeasures necessary for the protection of the system.

2.1 Identifying System Assets

Identification of system assets is necessary for determining system threats, vulnerabilities, and risks, and the appropriate level of security to apply to the system and related system components. System asset identification includes the following:

- Identifying and documenting the system architecture.
- Identifying system and subsystem assets, including all hardware, software, and ancillary equipment.
- Identifying system interfaces (external and internal).
- Identifying system boundaries.

Based on identification of the system assets, a system description is developed and documented in the Security Plan or Technical Architecture Document for complex systems. Once assets have been determined, system security needs are identified by first determining system sensitivity requirements and severity (impact of system loss) related to system information confidentiality, integrity, and availability. Federal IT security standards define the following three basic protection requirements in order to determine the information sensitivity:

1. **Confidentiality**: Protection from unauthorized disclosure.

2. **Integrity**: Protection from unauthorized, unanticipated, or unintentional modification. Also includes:
    - Non-repudiation: Verification of the origin or receipt of a message.
    - Authenticity: Verification that the content of a message has not changed in transit.
3. **Availability**: Available on a timely basis to meet mission requirements or to avoid substantial losses.

The system environment is defined by the system architecture and physical locations where the system is installed. The system environment includes the physical and electronic access to system assets or data for each type of site installation. The severity of impact is represented by the potential loss of confidentiality, integrity, and/or system availability, which affects system assets or data. This impact is measured by loss of system functionality, impedance, or inability to meet an Agency mission, dollar losses, loss of life, loss of safety, loss of public confidence, or unauthorized disclosure of data. The risk level is determined by evaluating system assets, system requirements, and the information stored, processed, or transported by the system. Risk level is determined by using a qualitative ranking of **high**, **moderate,** or **low** for system confidentiality, integrity, and availability. System assets will be assessed for sensitivity in Section 3.6.

2.2 Analyzing System Threats

Threat sources are any event, process, activity, or action with the potential to cause harm to a system or that exploits a vulnerability to attack an asset. It is any force or phenomenon that could degrade the confidentiality, integrity, or availability of an asset. The capabilities, intentions, and attack methods of hostile entities that have a potential to cause harm to the system must be identified and evaluated. A threat source is normally known, includes physical, natural, environmental, and human sources, and normally impacts most networks and computer systems when adequate safeguards have not been implemented. A threat source is defined as any circumstance or event with the potential to cause harm to an IT system or that exploits a vulnerability to attack an asset. It is any force or phenomenon that could degrade the confidentiality, integrity, or availability of an asset. The common threat-sources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include natural flood because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees; or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a Trojan horse program written to increase productivity through bypassing system security. The reason for bypassing security may be benign, but the effect is still to weaken system security. Threat agents or actions used in the risk assessments are based on the threats identified in NIST *Risk Management Guide for Information Technology Systems,* SP 800-30 . Although threats can be realized in various forms (i.e., threat agents), threats to systems, leased telecommunications systems, and public telecommunications services can be categorized into three main groups:

- **Natural Threats**: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

- **Human Threats**: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).

- **Environmental and Physical Threats**: Long-term power failure, pollution, chemicals, liquid leakage.

Telecommunications systems, networks, network management systems, computers, and information systems are vulnerable to many threats that can cause damage. The threat is viewed as the stimulus, the vulnerability is the weakness, and the impact is the net effect on the system or information processed, stored, or transmitted by the system. A threat can manifest itself in a number of ways, which are either known or unknown vulnerabilities. The end result of a threat capitalizing on any vulnerability creates a potential compromise of the agency's protected assets and information. Threats result in one or more of five general consequences: unauthorized disclosure, data corruption, or destruction, denial of service, system failure, and communications loss. These threats are analyzed in Table 2.1, Threats and Potential Impacts.

Table 2.1: Threats and Potential Impacts

	Threat	Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
	Natural Threats					
1	Fire/Smoke	An accidental or intentional fire could damage system equipment or facility.	√	√		
2	Acts of Nature	All types of natural occurrences (e.g., earthquakes, hurricanes, tornadoes) that may damage or affect the system.	√	√		√
3	Water Damage	Water from internal or external sources may damage system components.	√	√		
	Human Threats					
4	Espionage/Sabotage/Terrorism/Vandalism	Espionage is the intentional act of or attempt to obtain confidential information. Sabotage is premeditated destruction or malicious modification of assets or data for personal or political reasons. Terrorism is the destruction or damage of resources for political reasons. Vandalism is the destruction of system resources with no clearly defined objective.	√	√	√	√
5	Theft/Pilferage	Theft is the unauthorized removal of computer equipment or media. Pilferage is theft of property by personnel granted physical access to the property.	√			√
6	Hacking/Social Engineering	Software may be modified intentionally to bypass system security controls, manipulate data, or cause denial of service. Social engineering is the human-to-human interaction in which a hacker gathers data for use in modifying or manipulating the system.	√		√	√

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
7	Malicious Code	Malicious software such as viruses or worms may be introduced to the system, causing damage to the data or software.	√	√	√	√
8	User Errors/Omissions	Application and support system components may be inappropriately modified or destroyed due to unintentional administrator or user error.	√	√	√	√
9	Mismanagement/Waste	Losses and delays caused by failure to plan, failure to adhere to plans, policies or procedures.	√	√	√	√
10	Browsing/Disclosure	Intentional unauthorized access to confidential information by outsiders or by personnel with system access but not having a need to know (browsing)				√
11	Eavesdropping/interception	Intentional unauthorized access to confidential information through technical means (sniffing/interception) or by personnel having some level of system access but not having a need to know (eavesdropping)				√
12	Data Integrity Loss	Attacks on the integrity of system data by intentional alteration.			√	
13	Misuse/Abuse	Individuals may employ system resources for unauthorized purposes.	√	√	√	√
14	Fraud	Use of the system by authorized personnel for illegal financial gain.			√	

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
	Environmental and Physical Threats					
15	Power Disruption	A power failure or fluctuation may occur as the result of a commercial power failure. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).	√		√	
16	Strike/Work Stoppage	Adverse impact on operations due to planned, intentional acts based on organized employee dissatisfaction.	√			
17	Hardware/Equipment Failure	Failure or malfunction of hardware may cause denial of service to system users. Additionally, hardware configuration may be altered in an unauthorized manner, leading to inadequate configuration control or other situations that may impact the system.	√		√	√
18	Program Errors/Software Failure	Software malfunction or failure resulting from insufficient configuration controls (i.e., testing new releases, performing virus scans).	√	√	√	√
19	Communication Loss	Communication links may fail during use or may not provide appropriate safeguards for data.	√		√	√
20	Explosion/Bomb Threat	Intentional disruption of operations due to actual or threatened catastrophic explosion.	√	√		√
21	Chemical/Biological Incident	Disruption of operations and personnel hazards due to actual or potential effects of chemicals or biological agents to include infestations and illness.	√	√		

2.3 Analyzing System Vulnerabilities

Vulnerabilities are weaknesses in the environment, system architecture, design, or implementation; the organizational policies, procedures, or practices; and the management or administration of hardware, software, data, facility, or personnel resources. Vulnerabilities that are exploited may cause harm to the system or information processed, transported, or stored by the system. In accordance with NIST *Recommended Security Controls for Federal Information Systems*, SP 800-53, the vulnerability analysis encompasses the following three security control areas:

- **Management Controls** are safeguards related to the management of security of the system and management of the risk for a system. Examples of management vulnerabilities include lack of risk management, life cycle activities, system security plans, certification and accreditation activities, and security control reviews.

- **Operational Controls** comprise the operational procedures that are performed with respect to an information system. More often than not, these vulnerabilities stem from the lack of (or an insufficiency in) the various practices and procedures that are critical to the secure operation of a system. Examples of operational vulnerabilities include the lack of (adequate) security awareness and training, security monitoring and detection provisions, personnel and physical security controls and security auditing, and the absence of some or all of the procedural documentation critical to an effectively applied and managed security program.

- **Technical Controls** are countermeasures related to the protection of hardware, software, system architecture, and modes of communication. Examples of technical vulnerabilities include insufficient security software controls and mechanisms, faulty operating system code, lack of virus controls and procedures, and lack of authentication and access controls. Normally, vulnerabilities are identified during the risk assessment or during security testing and evaluation. In order to gain an understanding of the system vulnerabilities, major security certification activities include:

  - Developing a detailed data collection questionnaire.
  - Conducting site surveys and visits of representative installation sites.
  - Interviewing users and maintainers of the system.
  - Documenting findings.

After analyzing system management, operational, and technical security controls for the system in its fielded environment, system vulnerabilities are then identified.

The analysis of the system's vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation resulted in a risk rating for each missing or partially implemented control. The risk level was determined on the following two factors:

1. **Likelihood of Occurrence** - The likelihood to which the threat can exploit a vulnerability given the system environment and other mitigating controls that are in place.

2. **Impact** – The impact of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation or interest.

To determine overall risk levels, the analyst must first look at how important the availability, integrity, and confidentiality of the system is in relation to it being able to perform its function, and the types of damage that could be caused by the exercise of each threat-vulnerability pair. Exploitation of vulnerability may result in one or more of the following types of damage to a system or its data:

- **Loss of Availability/Denial of Service** – Access to the system, specific system functionality or data is not available (Asset is not destroyed).

- **Loss of Integrity/Destruction and/or Modification** – Total loss of the asset either by complete destruction of the asset or irreparable damage, or unauthorized change, repairable damage to the asset, or change to asset functionality.

- **Loss of Confidentiality/Disclosure** – Release of sensitive data to individuals or to the public who do not have a "need to know."

The analysis of the systems vulnerabilities and risk determination will be further discussed in Section 4.0, Risk Calculation.

3.0 System Description

3.1 System Description

Provide an overview of the system to include a system description and purpose. Document the system environment by including a description of hardware and software components, interconnectivity, locations and the user community. This can be extracted from the security plan for the system

3.2 System Name/Title

Insert System Name/General Support System or Major Application

3.3 Responsible Organization

Insert responsible organization name, department, division address

3.4 Information Contact(s)/System Owner

Insert Name
Insert Title
Insert Address
Insert Phone Number
Insert Email Address

3.5 Assignment of Security Responsibility

Insert Name
Insert Title
Insert Address
Insert Phone Number
Insert Email Address

3.6 Information Sensitivity

The information sensitivity for System Name is determined by using Step 2, "Classify GSSs and Applications," identified in HUD's *IT System Certification and Accreditation Inventory Guide*, April 2005. In accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, information sensitivity is calculated based on the three basic protection requirements: confidentiality, integrity, and availability.

The following table (Table 3.1) provides a general description of the information handled by the system and the need for protective measures.

Table 3.1: Information Categories

Information Category	Explanation and Examples	Protection Requirements
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Internal administration	Information related to the internal administration of HUD. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded

Information Category	Explanation and Examples	Protection Requirements
Investigation, intelligence, Critical Element related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence Critical Element related information that cannot be classified but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded

Information Category	Explanation and Examples	Protection Requirements
Mission-critical information	Information designated as critical to a HUD mission, includes vital statistics information for emergency operations.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Operational information	Information that requires protection during operations; usually time-critical information.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded

Information Category	Explanation and Examples	Protection Requirements
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
System configuration/ Management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at HUD; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded
Public information	Any information that is declared for public consumption by official HUD authorities. This includes information contained in press releases approved by the Public Affairs. It also includes Information placed on public access world-wide-web (WWW) servers.	• Confidentiality – describe why the confidentiality of system data needs protection • Integrity – describe why the integrity of system data needs protection • Availability – describe why the availability of the system must be safeguarded

In the following section, each protection requirement is rated on a scale of High, Moderate, or Low, using the guidance from NIST *Guide for Developing Security Plans for Information Technology Systems*, SP 800-18, and FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

The information sensitivity for System Name is as follows:

Confidentiality

Choose Appropriate Description of the Rating

High: The consequences of unauthorized disclosure or compromise of data or information in the system are **unacceptable**. Loss of confidentiality could be expected to cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Moderate: The consequences of unauthorized disclosure or compromise of data or information in the system are only **marginally acceptable**. Loss of confidentiality could be expected to cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Low: The consequences of unauthorized disclosure or compromise of data or information in the system are **generally acceptable**. Loss of confidentiality could be expected to cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals.

Integrity

Choose Appropriate Description of the Rating

High: The consequences of corruption or unauthorized modification of data or information in the system are **unacceptable**. Loss of integrity could be expected to cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Moderate: The consequences of corruption or unauthorized modification of data or information in the system are only **marginally acceptable**. Loss of integrity could be expected to cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or result

in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Low: The consequences of corruption or unauthorized modification of data or information in the system are **generally acceptable**. Loss of integrity could be expected to cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals.

Availability

Choose Appropriate Description of the Rating

High: The consequences of loss or disruption of access to system resources or to data or information in the system are **unacceptable**. Loss of availability could be expected to cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Moderate: The consequences of loss or disruption of access to system resources or to data or information in the system are only **marginally acceptable**. Loss of availability could be expected to cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Low: The consequences of loss or disruption of access to system resources or to data or information in the system are **generally acceptable**. Loss of availability could be expected to cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals.

3.7 Mission Criticality

The mission criticality for System Name is also determined by using Step 2, "Classify GSS's and Applications," identified in HUD's *IT System Certification and Accreditation Inventory Guide*, April 2005. The term **Mission Critical system** means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that:

- Is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

- Is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy.
- Processes any information, the loss, misuse, disclosure or unauthorized access to or modification of which would have a debilitating impact on the mission of an agency.

Non-Mission critical GSS's and applications are those automated information resources that do not fit under the mission critical definition and whose failure would not preclude the Department or a major subordinate organizational element from accomplishing core business operations in the short to long term, but would have an impact on the effectiveness or efficiency of day-to-day operations.

System Name is classified as a choose either **Mission Critical** or **Non-Mission Critical** system. This classification is based on the findings in Table 3.2 below.

Table 3.2: Protection/Certification Requirements

Concern	Ranking *(Low-Mod-High)*	Justification
Sensitivity		
Confidentiality		
Integrity		
Availability		
Certification Level of Effort	*Select either Low, Moderate, or High according to the highest sensitivity ranking above*	**Delete the two that do not apply** **Low =** Low intensity, checklist-based, independent security review • Interview of personnel • Review of system-related security policies, procedures, documents • Observation of system operations and security controls **Moderate** = Moderate intensity, demonstration-based, independent assessment • Functional testing • Regression analysis and regression testing • Penetration testing (optional) • Demonstrations to verify security control correctness and effectiveness • Low Certification Level verification techniques (if appropriate) **High** = High intensity, exercised-based, independent assessment • System design analysis • Functional testing with coverage analysis • Regression analysis and regression testing • Penetration testing (Red Team optional) • Demonstrations and exercises to verify security control correctness and effectiveness • Low and Moderate Certification Level verification techniques (if appropriate)

4.0 Risk Calculation

This section discusses vulnerabilities, the threats that can exploit those vulnerabilities, and the probable impact of that vulnerability exploited. System vulnerabilities are identified as required security controls that are not fully implemented. These are classified as vulnerabilities because the lack of required controls result in vulnerability that a threat can be exploited successfully.

The analysis of system vulnerabilities, the threats that can exploit those vulnerabilities, and the probable impact of that vulnerability exploitation resulted in a risk rating for each missing or partially implemented control. The risk level was determined based on the following two factors[1]:

1. **Impact** of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation, or interest.

2. **Likelihood** to which the threat can exploit a vulnerability given the system environment, threat frequencies, and other mitigating controls in place.

The following sections discuss the areas of potential impact and how the values for the above two factors, magnitude of impact and likelihood of occurrence, and the level of risk were determined. The factors used in these sections are derived from NIST *Risk Management Guide for Information Technology Systems,* SP 800-30.

4.1 Impact

An impact analysis prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. The system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. To determine overall risk levels, the analysis first looked at how important the availability, integrity, and confidentiality of the system and/or its data are to the ability of the system to perform its function and the types of damage that could be caused by the exercise of each threat-vulnerability pair. Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any of the three security goals: integrity, availability, and confidentiality.

To determine overall risk levels, the analysis first looked at how important the security goals (availability, integrity, and confidentiality) of the system and/or its data are to the mission's ability to function as intended. The system sensitivity values of this report were mapped to the magnitude of impact qualitative values of high (100), moderate (50), and low (10) as defined in the NIST guidelines and shown below in Table 4.1.

[1] Note that in many risk evaluations the following additional criterion is used: exploitation could result in human death or serious injury. Given the type of data processed by network and system functionality, compromise of the system could not result in death or injury.

Table 4.1: Definitions

Impact Level/Value	Impact Description
High (100)	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate (50)	Exercise of the vulnerability (1) may result in the costly loss of major tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (10)	Exercise of the vulnerability (1) may result in loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Exploitation of vulnerability by any of threats defined in section 2.2 may result in one or more of the following types of damage/impact to a system or its data as documented in Table 2.1 (Threats and Potential Damage):

- **Loss of Availability/Denial of Service**: Access to the system, specific system functionality, or data is not available (asset is not destroyed).
- **Loss of Integrity/Destruction and/or Modification**: Total loss of the asset either by complete destruction of the asset or irreparable damage, and/or unauthorized change, repairable damage to the asset, or change to asset functionality.
- **Loss of Confidentiality/Disclosure**: Release of sensitive data to individuals or to the public who do not have a "need to know."

Table 4.2 below shows the mapping of security goals (availability, integrity, and confidentiality) to the maximum threat impact values for the system as follows:

Table 4.2: Threat Impact and Security Sensitivity Mapping

Threat Impact Areas	System Sensitivity Values	Maximum Impact Value
Loss of Availability/Denial of Service	Availability (A) – Enter High, Moderate, or Low according to Section 3.6 above	Enter 100 for High, 50 for Moderate, or 10 for Low sensitivity
Loss of Integrity/ Destruction/Modification	Integrity (I) – Enter High, Moderate, or Low according to Section 3.6 above	Enter 100 for High, 50 for Moderate, or 10 for Low sensitivity
Loss of Confidentiality/Disclosure	Confidentiality (C) - Enter High, Moderate, or Low according to Section 3.6 above	Enter 100 for High, 50 for Moderate, or 10 for Low sensitivity

The impact of a specific threat exploiting vulnerability is determined by adding all applicable impact values for the given threat. The formula for Threat Impact is as follows:

Impact = A + I + C

Given the security sensitivity values for the environment, the total possible Impact value for the environment is 300. For example, if Threat #1 (Fire) is mapped to a specific vulnerability, the threat impact areas are Denial of Service and Destruction. Therefore, the impact value for the threat-vulnerability pair is 100. If multiple threats are applicable to a single vulnerability, the threat with the greatest number of impact areas is used to determine the overall impact value.

4.2 Likelihood of Occurrence

The likelihood that a threat will exploit a vulnerability and cause damage for each of the four areas listed above was determined based on the following factors: the frequency of the threat and the existence of mitigating controls. Likelihood of occurrence was determined qualitatively to be high, moderate, or low using the following criteria in Table 4.3:

Table 4.3: Likelihood of Occurrence Values Criteria

Value	Likelihood of Occurrence Description
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
Moderate	The threat-source is motivated and capable, but controls are in place that may impede successful exploitation of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.

In accordance with NIST guidelines, a numerical value was assigned for likelihood of occurrence as follows:

High = 1.0
Moderate = 0.5
Low = 0.1

Based on the threat frequency documented in section 3.6 (Information Sensitivity) and the value entered in the vulnerability questionnaire of "I" (Implemented), "P" (partial), "NI" (Not Implemented), and "N/A" (Not Applicable) a likelihood value is assigned to the threat-vulnerability pairs listed in the RA table using the mappings shown in Table 4.4.

Table 4.4: Assignment of Likelihood Values

Countermeasure Implementation Status	Threat Frequency		
	High (3)	Moderate (2)	Low (1)
I (Implemented)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1
P (Partially Implemented)	Likelihood = 0.5	Likelihood = 0.5	Likelihood = 0.1
NI (Not Implemented)	Likelihood = 1.0	Likelihood = 1.0	Likelihood = 0.5
NA (Not Applicable)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1

4.3 Risk Level

A relative risk level was determined for each vulnerability. The purpose in defining this risk level is to determine both the overall level of risk for the system as well as the degree to which each vulnerability contributes to that risk. The risk level for each control also serves as the basis for prioritizing controls for implementation.

The determination of risk for a particular threat/vulnerability pair can be expressed as a function of the likelihood of occurrence and magnitude of impact. The overall level of risk for each control was determined by the following formula:

Risk = Likelihood x Impact

Table 4.5 indicates the range of possible risk values.

Table 4.5: Risk Level Matrix

Risk Level Range of Values						
Availability/Denial of Service		**Integrity/Destruction and/or Modification**		**Confidentiality/Unauth. Disclosure**		**Risk Level**
Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	
High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	
1	100	1	100	1	100	300
0.5	50	0.5	50	0.5	50	75
0	1	0	1	0.1	10	3

As illustrated in the table 4.5 above, three is the lowest possible value for risk, 75 is the median value, and 300 is the highest possible value using this methodology.

Table 4.6 below shows the possible risk ranges for the system. Given the sensitivity values for the environment, the maximum possible risk value is 300, which falls in the high level of risk.

Table 4.6: Risk Value Matrix

Likelihood	Impact		
	Low (10)	**Moderate (50)**	**High (100)**
High (1.0)	Low 10 x 1.0 = 10	Moderate 50 x 1.0 = 50	High 100 x 1.0 = 100
Moderate (0.5)	Low 10 x 0.5 = 5	Moderate 50 x 0.5 = 25	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Moderate 50 x 0.1 = 5	High 100 x 0.1 = 10

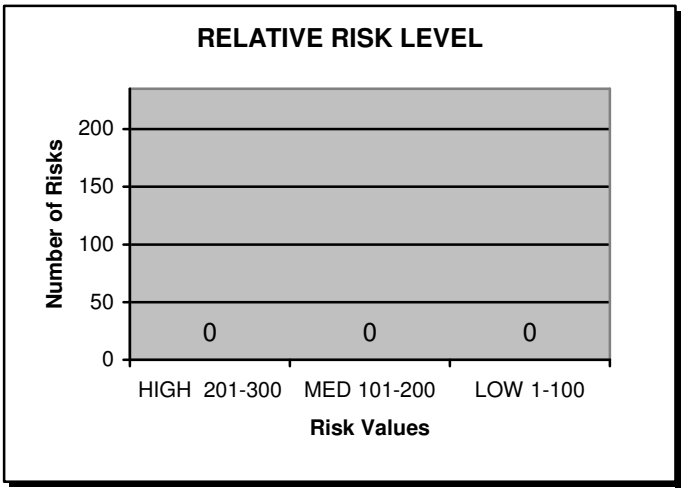
Risk Scale: Low (1 to 99), Moderate (100 to199), and High (200 to 300)

5.0 Risk Assessment Results

5.1 Risk Summary

Table 5-1 provides the risk assessment results for System Name. The following figure summarizes risk assessment findings as documented in Table 5.1:

Table 5.1: Relative Risk Level



The results of the risk assessment of System Name indicated that the primary risks to system resources related to unlawful/unauthorized acts committed by hackers, computer criminals, and insiders related to system intrusion, fraud, and spoofing. Unintentional user errors and omissions is an additional critical risk to system data and operations.

The assessment found that identified risks could be fully mitigated through the implementation of security controls specified in the System Name Security Plan and in the accompanying Plan of Action and Milestones.

5.2 Applicability of Minimum Security Baseline

The risk assessment of the System Name included an assessment of the applicability of the HUD Minimum Security Baseline to determine its adequacy in protecting system resources. Based on risks identified the assessment identified the controls shown in Table 5.2, which proved to be not applicable to System Name.

Table 5.2: Non-Applicable Controls

	Non-Applicable Controls	Justification
Management Controls		
Operational Controls		
Technical Controls		

5.3 Additional Controls Required

In addition to controls identified in the HUD Minimum Security Baseline (NIST SP 800-53), the risk assessment identified several additional controls that should be implemented to mitigate risks to System Name resources. These controls are shown in Table 5.3 below.

Table 5.3: Additional Controls

	Additional Controls	Justification
Management Controls		

	Additional Controls	Justification
Operational Controls		
Technical Controls		

Table 5.1: System Name Risk Matrix (SAMPLE)

NUMBER	SECURITY CONTROL	THREAT	STATUS	Availability (Denial of Service)		Integrity		Confidentiality (Disclosure)		RISK FACTOR	RISK
				Likelihood	Impact	Likelihood	Impact	Likelihood	Impact		
			I,P,NI, ACCEPT RISK	High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	High = 1 Med = .5 Low = .1	High = 100 Med = 50 Low = 10	High=201-300 Med=101-200 Low =1-100	
1	SA-2 Allocation of Resources: The organization has not determined, documented, nor allocated as part of its capital planning and investment control process the resources required to adequately protect the information system.	All Threats	P	0.5	50	0.5	50	0.1	100	60	Low
2	CA-7 Continuous Monitoring: The organization does not monitor the security controls in the information system on an ongoing basis.	All Threats	I	0.1	50	0.1	50	0.1	100	20	Low
3	**PS-3** Personnel Screening**:** The organization does not screen individuals requiring access to organizational information and information systems before authorizing access.	Fraud	NA	0.1	50	0.1	50	0.1	100	20	Low
4	**MA-4** Remote Maintenance**:** The organization does not approve, control, or monitor remotely executed maintenance and diagnostic activities.	Unauthorized Access	NI	1.0	50	1.0	50	1.0	100	200	High

INDEX