Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS INFORMATION SECURITY RISK ASSESSMENT (IS RA) PROCEDURE

March 19, 2009

Version1.0- Final

Summary of Changes in IS RA Procedure Version 1.0

1. This document replaces the *CMS Information Security Business Risk Assessment Methodology,* dated May 11, 2005 and the *CMS Information Security Risk Assessment Methodology,* dated April 22, 2005. The CMS lifecycle framework will now combine the Business RA and Information Security (IS) Risk Assessment, processes into one procedure which addresses both business and system risks.
2. Section 1.1 Overview. This section is reworded to be consistent with the IS documentation and introduces the documents the Business Owner and/or System Developer/Maintainer must integrate for a successful IS RA process.
3. Section 1.2 Purpose. This section is changed to reflect "Scope". The change to scope will align the CMS IS RA Procedure with the standard introduction contents (1.0 Introduction, 1.1 Overview, 1.2 Scope, and 1.3 Roles and Responsibilities) of the CMS program documents.
4. Section 1.3 Roles and Responsibilities. Add this section to provide the CMS roles that are responsible for the IS risk management/assessment process.
5. Section 2.0. Added the IS RA process flow to this section.
6. Section 2.0. Created IS RA Interfaces figure.
7. Inclusion of Appendix B – Moved E-authentication assurance levels determination process to an appendix.
8. Section 2.0. Inclusion of "Process" for consistency with former Business RA and IS RA methodologies.
9. Deletion of "Scope".
10. Inclusion of System Security Plan Workbook(s) references and instructions.
11. Instructions specific to the Risks Table.
12. Inclusion of tables and examples from both the Business and IS RA documents.
13. Inclusion of Appendix: D References.
14. Inclusion of Appendix: E Abbreviations/Acronyms.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document replaces the Centers for Medicare & Medicaid Services (CMS) *Information Security Business Risk Assessment Methodology*, dated May 11, 2005 and the *CMS Information Security Risk Assessment Methodology*, dated April 22, 2005. The CMS Integrated IT Investment & System Life Cycle Framework here after referred as "Framework" will now combine the Business Risk Assessment (RA) and Information Security (IS) RA processes into one procedure, which addresses both business and system risks. The *CMS Information Security Risk Assessment (IS RA) Procedure* is developed to provide the CMS Business Owners with the tools to continuously identify and mitigate business and system risks throughout the life cycle of the General Support System (GSS) or subsystem, or Major Application (MA) or MA individual application.

Risk Management (RM) is an essential function that is iterative within the life cycle of the Business Owner's GSS or MA. RM is performed by the Business Owner to ensure adequate resources, policies, procedures, processes, and practices are in place. The Business Owner performs RM to identify and assess risk exposures, understand the system environment, perform risk analysis on data collected, and monitor risk mitigation activities to ensure the IS RA processes implemented are performed adequately. The RM functions minimally performed by the Business Owner include the following:

- Operational Planning;
- Ongoing Data Collecting;
- Risk Analysis; and
- Monitoring and Measuring Risks.

The general roles and responsibilities that govern the implementation of the Business Owner's IS RA are provided within this document as well as a life cycle phase-by-phase description of the activities the Business Owner should be aware of and perform at each phase of the "Framework". An IS RA Checklist is provided in Appendix C. In addition, steps and processes to undertake when a business or system risk is identified are provided for the Business Owner working with their System Developer/Maintainer and Information System Security Officers (ISSO), which consist of the following:

- Document Business Function/System Purpose and Description;
- Conduct Risk Determination;
- Conduct Safeguard Determination; and
- Conduct Safeguard Implementation.

The CMS IS RA Procedure provides instructions for completing an IS RA. The Business Owner shall complete the CMS IS RA Template to ensure an accurate identification, capture, and communication of both business and system risks that require mitigation. The IS RA is an essential component of the CMS IS Model. This document provides an overview of the interfaces between the IS RA and the following:

- *CMS Policy for the Information Security Program (PISP);*

- *CMS Information Security (IS) Acceptable Risk Safeguards(ARS) including the CMS Minimum Security Requirements (CMSR) [Low, Moderate, High];*
- *CMS IS Certification and Accreditation (C&A) Program Procedure;*
- *CMS System Security Level by Information Type;*
- *CMS System Security Plan Workbooks [Low, Moderate, High and E-authentication];*
- *CMS System Security Plans (SSP) Procedure; and*

1. INTRODUCTION

1.1. OVERVIEW

The *Centers for Medicare & Medicaid Services (CMS) Information Security Risk Assessment (IS RA) Procedure* presents a systematic approach for the identification, and mitigation of both business and system risks. An IS RA shall be prepared for each General Support System (GSS), GSS sub-system (if applicable), Major Application (MA), and MA individual application. The IS RA contains a list of system threats and vulnerabilities, an evaluation of current system security controls, their resulting risk levels, and any recommended safeguards to reduce the system's risk exposure. The IS RA also supports risk management through the evaluation of the system's risk impact upon the CMS enterprise-wide IS model.

These Procedures are promulgated under the legislative requirements set forth in the Federal Information Security Management Act of 2002 (FISMA) and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*. Federal law requires CMS to implement a risk-based program for cost-effective IS. All business processes operate with some level of risk and one of the most effective ways to protect these business processes is through the implementation of effective internal security controls, risk evaluation, and risk management (RM).

To manage a risk-based IS program, Business Owners are responsible for adhering to and implementing the policy and procedures contained within the following CMS enterprise-wide IS Program documents found at https://www.cms.hhs.gov/informationsecurity including but not limited to the following:

- *CMS Policy for the Information Security Program (PISP);*
- *CMS Information Security Acceptable Risk Safeguards (ARS) including the CMS Minimum Security Requirements (CMSR) [High, Moderate, Low];*
- *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedure;*
- *CMS System Security Plan (SSP) Procedure;*
- *CMS Information Security Contingency Plan Procedure; and*
- *CMS Information Security Assessment Procedure.*

1.2. SCOPE

The IS RA shall provide details pertaining to business and system risks that are identified during the phases of the "Framework". Business risk details provide decision-makers with the information required to understand the impact of interruptions on business functions and outcomes. System risk details allow for the analysis of the system's security posture in the light of ever changing technologies and potential security threats. The analysis of both business and

system risks serves as a basis for informed judgments concerning the extent to which action is needed to reduce the level of risk present in both the business processes as well as the information system.

The RA identifies potential threat/vulnerabilities in the information system, analyzes planned or actual security controls and potential impacts on operations, assets, or individuals, and determines expected risk. For new systems, or technical environments undergoing a major modification, security requirements shall be included in the Baseline Requirements Document that is produced as part of the Requirements Phase of the "Framework" as well as maintained and updated as needed throughout the life cycle. The products of an assessment is the identification and documentation of additional safeguards required for protecting and preserving the Confidentiality, Integrity, and Availability (CIA) of the CMS business function and the information system and an assessment of the residual risk level once the additional or different safeguards are implemented.

The *CMS IS RA Procedure* is a tool to guide Business Owners in conducting an IS RA. The IS RA is incorporated into the SSP and is reviewed during the CMS Certification and Accreditation (C&A) process. The *CMS IS RA Procedure* presents information in two parts: 1) identifies the RA and RM activities that take place during phases of the "Framework", and 2) defines the steps and processes when a business or system risk is identified. The IS RA Procedure supports RM in the evaluation of the business functions and the system risk impact upon CMS' enterprise IS model. CMS requires each Business Owner to develop or update an IS RA in response to each of the following events:

- New system;
- Major business process or technology/system modification(s);
- Every third year of an operational system;
- Increase in security risks/exposure;
- Increase of overall system security level; and/or,
- Serious security violation(s) as described in the *CMS Information Security Incident Handling and Breach Analysis/Notification Procedure*.

1.3. ROLES & RESPONSIBILITIES

The following roles are responsible for various tasks, assignments, and deliverables throughout the RM process.

Table 1: Roles and Responsibilities

Role	Responsibility
CHIEF INFORMATION OFFICER (CIO)	The CIO is responsible for, but not limited to, the following: • Developing and maintaining information security policies, procedures, and control techniques that address system security planning; • Managing the identification, implementation, and assessment of common security controls; • Ensuring that IS RA training is developed as part of the

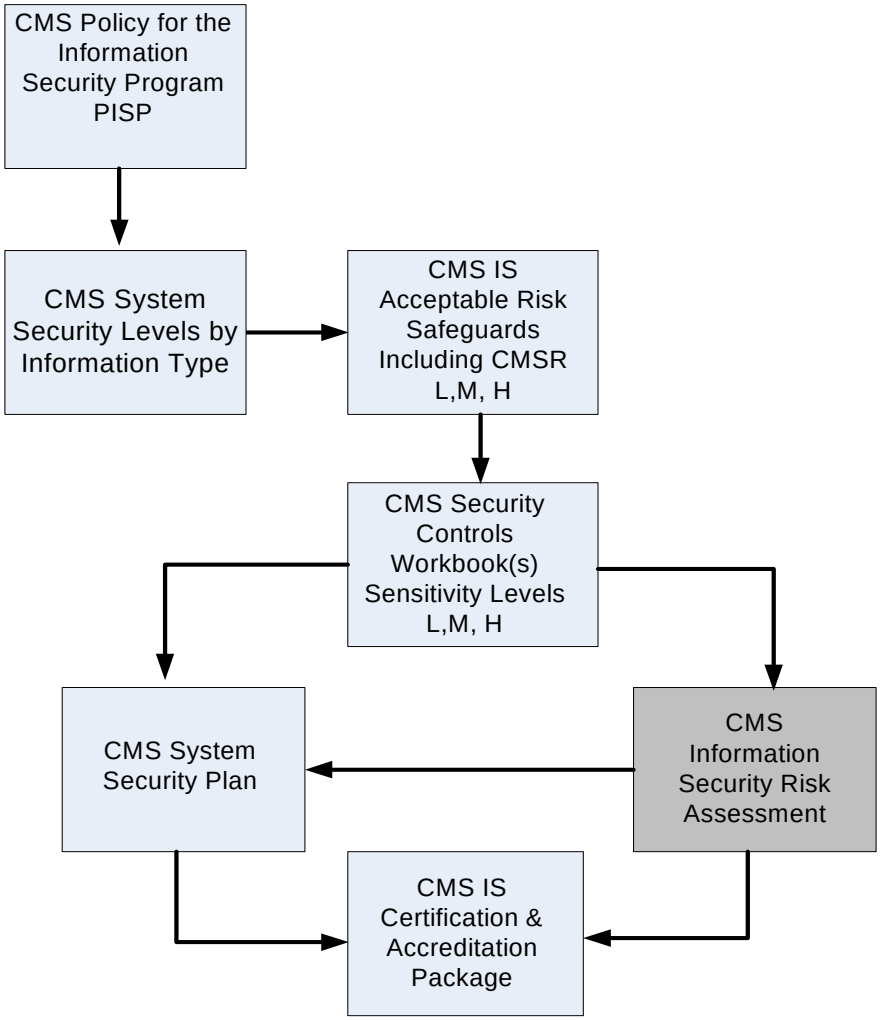
	security program and made available for the CMS Business Owners and System Developer/Maintainers responsible for developing and supporting an IS RA; and • Assisting senior agency officials with their responsibilities for IS RAs
CHIEF INFORMATION SECURITY OFFICER (CISO)	The CISO is responsible for, but not limited to, the following: • Carrying out the CIO's responsibilities for identifying the minimum information security controls, determining system security levels by type, and developing IS Program documents that support IS RA processes; • Advising Business Owners and System Developers/Maintainers on the CMS IS C&A Program and its implications for identifying risks; • Communicating the requirements for the development and review of IS RAs to the Business Owners, ISSO, and the authorizing officials; and • Coordinating the identification, implementation, and assessment of common security controls.
INFORMATION SYSTEM SECURITY OFFICER (ISSO)/ SYSTEM SECURITY OFFICER (SSO)	The ISSO/SSO is responsible for, but not limited to, the following: • Assisting the CISO in the identification, implementation, and assessment of the common security controls; • Playing an active role in developing and updating the IS RA as well as coordinating with the Business Owner for any changes to the system and assessing the security impact of those changes; and • Liaising between CISO and Business Owners on the CMS IS Program Requirements for their component systems.
BUSINESS OWNER	The Business Owner is responsible for, but not limited to, the following: • Developing and maintaining the IS RA and ensure that the system is deployed, and operating in accordance with the agreed-upon security requirements; • Updating the IS RA as required; • Assisting in the identification, implementation, and assessment of the common security controls; and • Developing the SSP that contains the detailed description of controls referenced in the IS RA.
SYSTEM DEVELOPER /MAINTAINER	The System Developer/Maintainer is responsible for, but not limited to, the following: • Developing the IS RA at the direction of the Business Owners and in coordination with the ISSO, CISO and other parties involved with the development of the

	system; and • Providing input and assist Business Owners regarding the security requirements and security controls for the information system(s) where the information resides.

1.4. IS RA INTERFACES WITHIN CMS SECURITY ENVIRONMENT

The IS RA Procedure are a set of processes and activities that must correlate with the development of a System. The RA processes are integrated within CMS processes and procedures defined in the IS environment. A summary depiction of the interfaces within the CMS enterprise-wide IS environment is depicted below in Figure 1: CMS IS RA Interfaces.

Figure 1: CMS IS RA Interfaces



A summary description of the interfaces is provided as follows:

- CMS PISP – Establishes the policy for the CMS IS program and the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents.
- CMS System Security Levels by Information Type – CMS has defined eleven (11) system security levels by information types. The CMS system security levels by information types is the first step taken by the Business Owner to define the system security levels by information types for their system. Once the level is established, the Business Owner will review the CMS IS ARS.
- CMS IS ARS – Contains the minimum level of security controls that must be implemented to protect CMS' information and information systems. The Business Owner will evaluate and document the expected minimum controls relative to the System Security Level of the system, as defined in the CMS IS ARS using the Security Controls Workbook.
- System Security Plan Workbook(s) – The workbooks provide the Business Owner with a list of security controls that represent the minimum controls that are required to be implemented based on the system sensitivity level (Low, Moderate, and High). The Business Owner will also utilize the System Security Plan Workbook(s) to support development of the SSP and IS RA.
- IS RA – The Business Owner must document and certify the incorporated security/internal controls are in place or the risks to the CIA for not complying with the requirement. The Business Owner will include the IS RA as part of the C&A package to support system certification and accreditation.
- SSP – The SSP contains a detailed description of controls that are in place to ensure the CIA of the system. The Business Owner will include the SSP as part of the C&A package to support system certification and accreditation.
- Certification &Accreditation (C&A) – The C&A package contains the necessary documentation to demonstrate and validate that appropriate security controls were implemented throughout the development of the system and exist to safeguard the system. The Business Owner will prepare the C&A package for the accreditation authority. (See *CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedure* for specifics).

The IS RA process described within this document is an integral part of RM. RM also includes prioritization of risks, categorization of recommended safeguards and the feasibility of their implementation, managing and tracking Corrective Action Plans (CAPs) and other risk mitigation processes and solutions within the business function, management, operational and technical areas. These RM activities are performed as part of the IS C&A process as it affects both the business function(s) and the system's security posture within the organization.

2. IS RA WITHIN THE CMS LIFE CYCLE

The RA Process is initiated when a system is identified within the "Framework". The CMS life cycle phases and related IS RA activities for the Business Owner to conduct are provided in this section. The IS RA should be developed, referenced and revised as the given system progresses through the CMS Integrated IT Investment & System Life Cycle Framework. The located at:

http://www.cms.hhs.gov/SystemLifecycleFramework

The goal of CMS' "Framework" is to provide a structure for managing a system throughout its life cycle from Initiation through Disposition including the incorporation of the appropriate protections of the information and the information system. However, an IS RA is not simply a paper exercise describing risks and safeguards, nor is it developed and then put aside. Information risks and vulnerabilities change as rapidly as the technology used to process the information. Security implementation must be a continuous process addressing risks, vulnerabilities, security controls and performing regular reviews throughout all stages of the system's lifecycle.

A properly developed and maintained IS RA is invaluable as it allows the organization to understand and monitor the effectiveness of the security controls. This procedure describes the steps necessary to produce a IS RA, which is reviewed during the CMS IS C&A process. The SSP process supports CMS' enterprise security model by providing a foundation for the evaluation of system-related security controls. Appendix A, *IS RA Template Instructions* includes directions on how to complete the IS RAs. In addition, the actual IS RA Template to be completed for all CMS systems can be found at:

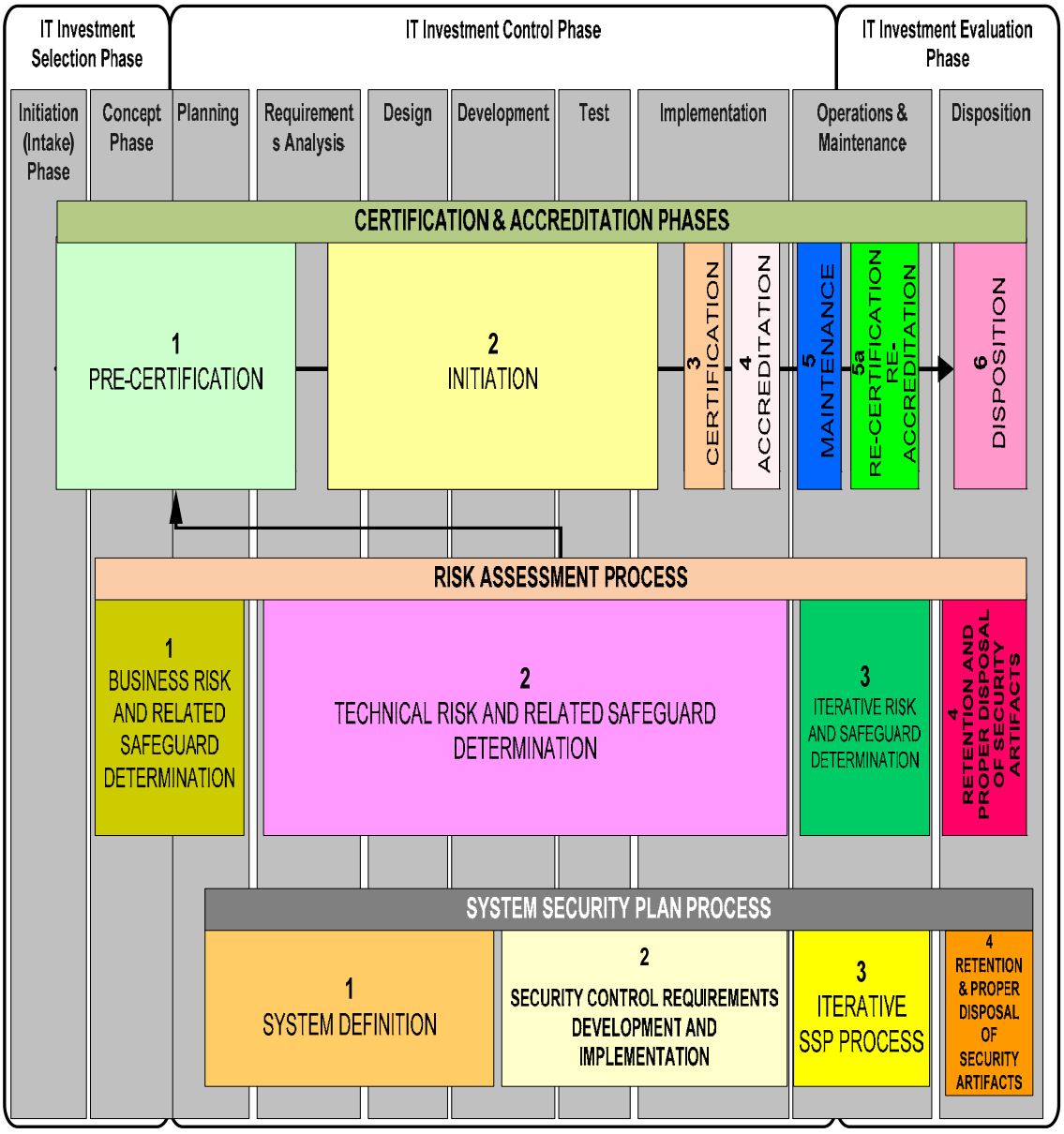
http://www.cms.hhs.gov/informationsecurity/downloads/ssp_template.doc

CMS business partners should review the "Framework" to assist them in describing in their respective IS RAs how their corporate life-cycle process / methodology implements IS. The CMS "Framework" can be found using the following URL:

http://www.cms.hhs.gov/SystemLife-cycleFramework/01_overview.asp

The CMS IS RA Process is initiated during the Concept phase within the "Framework" or from a C&A perspective in the Pre-Certification Phase of the C&A process. Figure 2 below depicts the CMS life-cycle phases and related IS RA activities followed by the detailed description.

Figure 2: CMS Life Cycle Phases and Related IS RA Activities



2.1. Phase 1 - Initiation (Intake)

The Business Owner during this phase works with the Office of Information Services (OIS) CISO to determine if the system is either a GSS or an MA and what FISMA system family controls will be applied. Once the Business Owner has obtained this designation, the identification of the System Security Level by Information Type is determined. Upon establishing this level, the Business Owner will review the CMS PISP and CMS IS ARS for the level of controls that must be employed in the system.

2.2. Phase 2 - Concept

At this phase of the life cycle, the Business Owner will begin to identify business risks and the initial draft of the IS RA is developed and then updated in subsequent phases. The business risks during this phase are defined as the vulnerabilities and threats that could be exploited and result in the loss of business functionality.

2.3. Phase 3 - Planning

The Business Owner reviews the minimum level of security controls contained in the CMS IS ARS and performs an evaluation of the controls to determine the appropriate level of controls for their system. The Business Owner will document the expected minimum controls relative to the sensitivity level of the system, as defined in the CMS IS ARS using the security controls workbook. Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy).

The Business Owner will initiate the development of the appropriate Security Controls Workbook for their system. The Business Owner will review the applicable system security level determination (Low, Moderate, or High) to select and initiate completion of the security controls workbook.

2.4. Phase 4 - Requirements Analysis

The Business Owner is responsible for the initial development of the SSP during this phase in concert with the continued development of the IS RA. Substantive development of both documents begins based on the security controls in the CMS PISP and CMS IS ARS and the utilizing the appropriate security controls workbook. These represent the controls that if not properly addressed will result in most of the system risks. Any business risks identified in the Phase 2: Concept or Phase 3: Planning are carried forward into the IS RA.

2.5. Phase 4 - Design

The IS RA is updated during this phase to account for any risks, vulnerabilities, and safeguards that have been identified or changed. The Business Owner shall follow the process depicted in Section 3.0 that forms a continuous RM practice. The SSP is also updated as needed during this phase. The SSP contains the detailed descriptions of controls that are in place for the system to ensure CIA.

Although these procedures address the IS RA the Business Owner needs to be aware of the symbiotic relationship with the SSP. While the IS RA captures the threats, vulnerabilities, and risks affecting the system, the SSP provides the detailed descriptions of all the implemented controls by the CMS IS ARS categories to minimize these risks. The Business Owner shall refer to the *CMS SSP Procedure* for details and instructions on completing the system SSP.

The Business Owner is responsible for ensuring the system requirements capture the business and security risks as applicable and have been translated into the effective system design to

protect the CIA of the CMS System. The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development.

2.6. Phase 6 - Development

The IS RA is updated during this phase to account for any risks, vulnerabilities, and safeguards that have been identified or changed as the development process progresses.

2.7. Phase 7 - Test

The IS RA is updated during this phase to account for any risks, vulnerabilities, and safeguards that have been identified or changed. The Business Owner shall identify an independent organization to conduct a Security Test and Evaluation (ST&E) based on the IS RA and the accompanying SSP. The independent ST&E is a technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures) and expected test results as defined in the *CMS Information Security Assessment Procedure*. The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls operate as defined, meet the approved security specification for the software and hardware, and implement the organization's security requirement. As necessary, the Business Owner shall identify corrective actions and report the results according to the *CMS Reporting Procedure for IS Assessments* and the *CMS Plan of Action and Milestone Procedure.*

The RM process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding identified risks must be made prior to system operation.

2.8. Phase 8 - Implementation

The IS RA is finalized in the Implementation Phase and is input to the C&A Package. The C&A will occur in the Implementation Phase. The Business Owner may continue to update the IS RA until the C&A process begins the C&A Package will contain the most current IS RA information. In addition, the Business Owner will finalize the SSP for submission with the C&A Package. The Business Owner will present the C&A package to the CIO through the CISO for accreditation according to the *CMS C&A Program Procedure* and the specific presentation requirements as defined in the *CMS SSP Procedure*. The CIO may provide a signed system accreditation, a conditional authority to operate, or deny operation of the system until certain corrective actions are taken.

2.9. Phase 9 - Operations and Maintenance

The Business Owner on an as needed basis updates the IS RA. In addition, the Business Owner as needed revises the C&A package documentation. A system re-certification and re-accreditation is conducted every three years for approval by the CIO or when there is a major

modification to the system, the system security level has changed, or a major security control has been compromised. The Business Owner shall conduct annual Security Controls Testing (SCT) and annual Contingency Plan (CP) testing and all identified risks or findings must be used to update the IS RA. RM activities are performed for periodic system reauthorization or whenever major changes are made to an IT system in its production environment (e.g., new system interfaces).

2.10. Phase 10 - Disposition Phase

During this phase, the Business Owner updates the IS RA as needed to reflect changes in the environment of the system. RM activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner. During this phase, the system and components are archived and must be maintained for three (3) years after the system is declared retired. The maintained requirement is for IS records purposes only as defined by National Archives and Records Administration (NARA) Schedule 24 and is not intended to supersede or circumvent established requirements for longer retention periods.

3. RISK MANAGEMENT

RM is performed by the Business Owner to ensure adequate resources, policies, procedures, processes, and practices are in place. RM is an essential function that is iterative within the "Framework" of the Business Owner's GSS or MA. The Business Owner shall; (1) plan for use of technology, (2) assess the risk associated with technology, (3) decide how to implement the technology, and (4) establish a process to measure and monitor risks.

3.1. OPERATIONAL PLANNING

Operational planning shall identify and assess risk exposure to ensure policies, procedures, and controls remain effective. IS RA is required as part of the CMS IS program. The assessments should address the CIA of the system, implemented security controls, and any foreseeable internal and external threats to the information, the likelihood of the threats, and the sufficiency of policies and procedures to mitigate the threats. Business Owners need to consider the results of these assessments when overseeing operations.

RM should cover all managerial, operational, and technical functions including business continuity. Business Owners should ensure Information Technology (IT)-related risk identification and assessment efforts at the system level are coordinated and consistent throughout the system FISMA family. An effective RM process will improve policy and internal control decisions within the system family. Business Owners can use RA data to make informed risk management decisions based on a full understanding of the managerial, operational, or system risks. Regardless of the complexity, the process should be formal and should adapt to changes in the IT environment.

3.2. ONGOING DATA COLLECTION

The Business Owner's understanding of the system environment is the first step in any RM process. Business Owners via the System Developer/Maintainer should incorporate information on IT issues during the RM process such as resource limitations, threats, priorities, and several potential locations that would include the following:

- IT strategic plans provide insight into the organization's planning process. Review and analysis of the strategic plans as part of the risk assessment process may spotlight developing risk exposures or other deficiencies that limit the institution's ability to implement strategic priorities;
- Business recovery and continuity plans prioritize the availability of various business lines to the institution and often encompass restoration and provision of control, customer service, and support. The plans can offer insight into the organization's critical operating systems and the control environment;
- IT help desk issue tracking reports can often indicate potential performance or control issues if the problem reports are aggregated and analyzed for repetitive or common issues; and
- Self-assessments on security controls (e.g., SCTs) can provide early identification of policy noncompliance or weaknesses in controls.

3.3. RISK ANALYSIS

The Business Owner should use the data collected on IT assets and risks to analyze the potential impact of the risks on the system and business functions. The analysis should identify various events or threats that could negatively affect the system strategically or operationally. The Business Owner should evaluate the likelihood of various events and rank the possible impact. Some examples of events that could affect the system are as follows:

- Capacity shortages – Shortages in capacity can result from lack of adequate hardware or network resources, including the lack of accurate forecasts of growth;
- External events – Systems may be exposed to external threats including weather-related events, earthquakes, terrorism, cyber attacks, cut utility lines or wide spread power outages that bring about system or facility failures;
- Security breaches – Security breaches that can affect the system include external and internal security breaches, programming fraud, computer viruses, or denial of service attacks;
- Systems development and implementation problems – Common system development and implementation problems include inadequate project management, cost/time overruns, programming errors (internal/external), failure to integrate and/or migrate successfully from existing systems, or failure of system to meet business requirements;
- System failures – Common causes of system failures include interdependency and interface failure, hardware failure, software failure, or internal telecommunication failure; and
- Technology investment mistakes – Mistakes in technology investment including strategic platform or supplier risk, inappropriate definition of business requirements, incompatibility with existing systems, or obsolescence of software may constrain the ability of the

functions to be performed and therefore the services intended to be provided are not adequate.

3.4. MONITORING

Business Owners should monitor risk mitigation activities to ensure identified objectives are complete or in process. Monitoring should be ongoing, and System Developers/Maintainers should provide progress reports to the Business Owners. Ongoing monitoring further ensures that the RA process is continuous instead of a one-time or annual event. The Business Owner should utilize their staff resources (System Developers/Maintainers, ISSO, etc.) to implement an effective monitoring process that minimally includes the following:

- Business Owner reporting;
- Clear assignment of responsibilities and accountability; and
- Mitigation or corrective action plans.

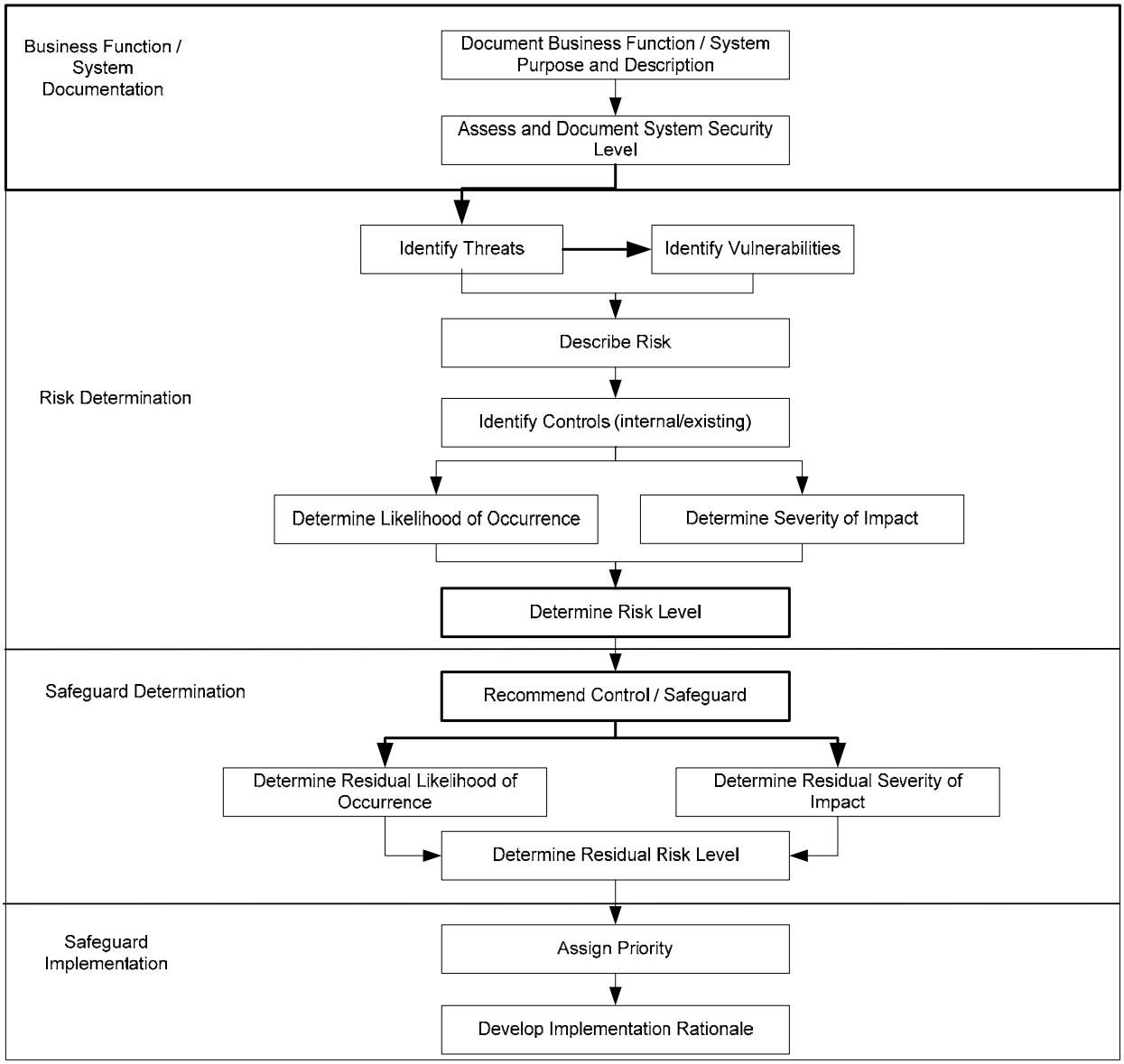
4. IS RA PROCESS

The CMS IS RA processes are iterative processes that continue throughout the "Framework". Security and technology controls result from an effective RA process. Therefore, the ability to mitigate risks is dependent upon a RA. The Business Owner should identify, measure, control, and monitor technology to avoid risks that threaten the functionality of the system.

4.1. IS RA PROCESS OVERVIEW STEPS

The Business Owner shall review and utilize the steps and processes defined in this section and Appendix A, IS RA Template Instructions to develop an IS RA. In addition, the Business Owner shall utilize the *CMS IS RA Template* to complete an IS RA for their respective GSS, GSS subsystem, MA, and MA individual application. The steps to identify a risk during the life cycle are grouped into four (4) distinct processes to form a continuous RM practice. Each process has individual objectives and tasks, and completion of each successive process depends upon the output of the preceding one. A checklist is provided in Appendix C, IS RA Activities Checklist. Although each process is depicted to be distinct and sequential, in practice some can be implemented in a Rapid Application Development (RAD) situation. An overview depiction of the RA processes and associated steps is provided below in Figure 3; IS RA Processes.

Figure 3: IS RA PROCESSES



To identify potential threats and associated vulnerabilities that may cause harm to, or disrupt the business functions and/or the system and are therefore identified as a risk, the Business Owner should perform the following:

- Review operational planning documents;
- Review ongoing data collection results;
- Review risk analysis performed by the System Developer/Maintainer; and
- Review monitoring reports.

For each potential threat/vulnerability pair, the Business Owner must determine the severity of impact upon the business function and/or the system's CIA, and determine the likelihood of the vulnerability being manifested within existing security controls. The product of the likelihood of occurrence and the impact severity results in the risk level for each threat to the business

function/system. Once the risk level is determined for each potential threat and vulnerability, safeguards shall be identified. Business risks and safeguards shall be developed for all levels of risk (low, moderate and high). System risks and safeguards shall be developed only for moderate and high-risk levels. Once the recommended safeguards have been implemented, the risks shall be re-evaluated to determine the remaining risk, or residual risk level.

In addition, the IS RA process shall determine the required level of assurance for electronic transactions and measure the relative severity of potential harm to CMS and/or business partners and other transaction participants in the event of an improperly validated or unauthorized authentication.

4.2. BUSINESS FUNCTION/SYSTEM DOCUMENTATION PROCESS

The Business Function/System Documentation process is the first process implemented when a risk is identified in the "Framework". This process provides background information that describes the following:

- The system and the data that is processed;
- Each business function supported by the system; and
- The business resources and information used in supporting each function.

TASK 1: INITIATION OF THE IS RA

The initiation of IS RA is the first task in the process. The objective of this task is to:

- Determine the applicable CMS System Security Levels by Information Type;
- Complete the applicable System Security Plan Workbook; and
- Prepare initial draft IS RA.

The Business Function/System Documentation process is designed to identify those areas in which the business and system functions are most at risk, and describe the safeguards in place or needed to protect those areas.

Task 1 Activities:

1. Assess the information processed by the system;
2. Document the business processes and technical environment;
3. Establish system security l level by information type;
4. Determine E-authentication Assurance Level;
5. Complete the Security Controls Workbook; and
6. Define technical requirements and operational practices.

4.2.1 DESCRIPTION OF BUSINESS FUNCTION AND SYSTEM

The Business Owner must provide system identification to include system description, business function/and assets, and system security level. For new systems, these are defined when the system is first conceived and developed during the "Framework" Design and Development Phases of the system. In addition, this section may be populated with information pertaining to an "anticipated" system, and updated accordingly once the system has been developed.

The Business Owner shall provide a statement describing the following:

- Each business function;
- Business processes supporting the function;
- Any interdependencies on other CMS business processes;
- A description of the technical environment expected to support the business process;

- An assessment of the sensitivity level of the information to be used in the business process; and
- An assessment of the criticality level of the business function.

4.2.2 SYSTEM SECURITY LEVEL ASSESSMENT

System security level designations are used to define the requirements of security efforts to protect CMS information and information system assets. Some of CMS' most critical information assets are the data residing within a system, such as financial, patient, and proprietary vendor data. Business Owners must determine the appropriate system security level based on the CIA of the information, as well as its criticality to the agency's business mission. This determination provides the basis for assessing the risks to CMS operations and assets in selecting appropriate security controls and techniques.

The *CMS System Security Level by Information Type* documents the categories of information that support the system and classify the system security level as Low, Moderate, or High. The *CMS System Security Level by Information Type* document can be downloaded from this link, http://www.cms.hhs.gov/informationsecurity.

4.2.3 DETERMINE E-AUTHENTICATION ASSURANCE LEVEL

Any CMS system/application that allows controlled individual web-based access, including Internet, Intranet or Extranet to conduct transactions must have an E-authentication assurance level. A transaction is an activity or request that updates one or more master files and serves as both an audit trail and history for future analyses. Ad hoc queries are a type of transaction as well, but are usually just acted upon and not saved (the master files are not updated). Indicate the E-authentication Assurance Level section within the IS RA template. Indicate if Resource Access Control Facility (RACF), Top Secret, Active Directory, or an equivalent authenticating mechanism is implemented for E-authentication of web-users, check the appropriate box. A detailed description of the E-authentication assurance levels is provided in Appendix B, E-authentication Assurance Levels. If the system does not have web-based transactions, proceed to the Risk Determination Phase (Task 2).

4.2.4 SYSTEM SECURITY PLAN WORKBOOK

Business Owners are strongly encouraged to complete the System Security Plan Workbook. The System Security Plan Workbook(s) provide the Business Owner with a list of security controls that represent the minimum controls required for the system based on the system security level. These controls are based on the CMS IS ARS. Commensurate with the CMS IS ARS, four (4) System Security Plan Workbooks have been developed that correspond to the three (3) system sensitivity levels, i.e., Low, Moderate, and High and one for E-authentication. The level of sensitivity of the system is driven by the *CMS System Security Level by Information Type*. The appropriate Workbook should be completed thoroughly, and in its entirety, as a part of the overall IS RA effort. For new systems, the Workbook should be completed once the system security level is determined. For existing systems, the Workbook should be completed when significant changes are made to a system and its security controls or when there is a change in

the systems security level or when a system is being re-accredited. These Workbooks will prove to be an invaluable resource that can be utilized during audits in developing security related documentation (IS RA and SSP) and be referenced when there is a change in system personnel.

System Documentation Process Milestone:
All system identification information has been captured.

4.3. RISK DETERMINATION PROCESS

The Risk Determination process is the second process of the IS RA process. This process calculates the level of risk for each potential threat and vulnerability to the business function/system based on the likelihood of threat occurrence or threat exploiting the vulnerability. This process also identifies the severity of impact that the threat occurrence or the exploited vulnerability would have on the system, its data, and its business function in terms of loss of CIA.

The Risk Determination Process comprises seven steps:

1. Identify threat/vulnerabilities.
    a. Identify potential threats to the business function, information, information systems and supporting business processes and resources that could affect the availability and functionality of the system.
    b. Identify the system weaknesses that could be exploited associated with the threat/vulnerability pair.
2. Analyze the potential impact of each threat to the business function to determine risk.
3. Analyze the potential CMS business impact of each risk.
4. Identify existing controls to reduce the risk of threat occurrence or for a threat exploiting a related vulnerability.
5. Determine the likelihood of a threat occurrence or a threat exploiting a related vulnerability given the existing controls.
6. Determine the severity of impact on the business/system function by threat occurrence or by an exploited vulnerability.
7. Determine the Risk Level given the existing controls.

This process will initially state the threats and the business risks identified during the investment analysis stage for new systems. If new business risks/vulnerabilities are identified that were unknown during the investment analysis stage, they should also be evaluated and added as a part of this IS RA process. For systems in development/production, the Business Owner will identify and analyze system threat/vulnerability pairs and determine if the level of risk has changed because of system level requirements or changes in technologies.

SCT is conducted annually on at least one third of the seventeen (17) security controls. If a security incident finding was identified then the Business Owner must capture the security incident as part of the Plan of Action and Milestone (POA&M) and develop a CAP. This information must further be included in the IS RA.

TASK 2: COMPLETE THE RISK DETERMINATION ITEMS WITHIN THE RISKS AND SAFEGUARDS TABLE

The objective of this task is:

- Update the IS RA by calculating the level of risk for each potential threat and vulnerability to include specific risk information. To accomplish this, the author must update the Risks and Safeguards Table.

Task 2 Activities:

1. Document the business function.
2. Document the threat to the business functions/systems.
3. Document the vulnerabilities for the system.
4. Provide the risk description, business impact and existing controls.
5. Provide the likelihood of occurrence and impact severity.
6. Calculate the risk level.

4.3.1 IDENTIFY AND DEFINE THE BUSINESS FUNCTION

A system can support one or more business functions. Examples of business functions of a system or application are data warehousing, call center operations, print fulfillment and Individual Voice Recognition (IVR) Transcription. Each business function has its own specific processes and associated controls. Another example is that of an accounting system with Accounts Payable, Payroll, and General Ledger business functions.

4.3.2 IDENTIFY THE THREAT

The Business Owner should identify threats that could have the ability to exploit system vulnerabilities. The Business Owners should categorize threats to the CIA for the GSS or MA in the following categories:

- Environmental/Physical;
- Human;
- Technical; and
- Natural.

The Business Owner where at all possible should group the threats by the mitigations that will reduce the affects of the threats against the system, business functions, supporting business processes, and resources. Refer to Table 2, Sample Business Threat Identification for examples of potential threats to a business function. The Business Owner must consider interdependencies with other business functions that may introduce new threats to the business function under review, as well as business rules that govern completion of the business function, including manual processes. Therefore, an understanding of the business function interdependencies and subordinate processes, if any, must be identified in this section. Such an understanding will provide significant information regarding inherited and new risks and controls that may affect the business function of the system as well as “up stream” or “down stream” systems.

Table 2: Sample Business Threat Identification

Threats	Threats Description	Examples

Threats	Threats Description	Examples
Data feed unavailable	Data required to complete the business function will not flow to the business processes.	Social Security Administration communications interrupted.
Key personnel unavailable	Personnel upon whom the business function relies are not available.	Medicare customer service representatives not available.
Access to workplace denied	Building contamination has resulted in complete closure of the facility.	A threat of biological contamination in the Mail Room has been detected.
Internal data network equipment is disabled or destroyed	An Agency-wide failure of data network services occurs resulting in the loss of Internet, Intranet, e-mail, fax, and other outside connectivity.	A major power fluctuation destroys the Agency's primary and secondary data network equipment.

4.3.3 IDENTIFY THE VULNERABILITY

For threats to the information system, vulnerabilities associated with each threat must be identified resulting in a threat/vulnerability pair. Vulnerabilities may be associated with either a single or multiple threats. Previous risk assessment documentation, audit and system deficiencies reports, security advisories and bulletins, automated tools, and technical security evaluations may be used to identify threats and vulnerabilities. Testing results during and after system development as part of the system's "Framework" may be used to identify vulnerabilities for new systems or systems undergoing major modifications.

4.3.4 DESCRIBE THE RISK

The risk description will include both the business risks and the system risks. For each potential threat to the business function and information system identified, develop one or more risk descriptions of how the business function may be affected adversely if the threat were to occur or business rules were circumvented. The risk description shall include the threat and describe specifically the impact to the business function that may result, if the threat is realized. A listing of sample risk descriptions is provided in Table 3; Sample Risk Descriptions, Business Impacts, and Existing Controls.

For the system risks, describe how the vulnerability creates a risk in the system in terms of CIA elements that may result in a compromise of the system and the data it handles. Complete the field labeled "Risk Description" in the "Risks and Safeguard Table" with the results of this step.

4.3.5 DETERMINE THE BUSINESS IMPACT

The business impact analysis is developed to determine the impact that could occur should the system be compromised. The following parameters should be considered for business impact analysis in which a negative impact of an event could result:

- Inconvenience, distress, or damage to standing or reputation;
- Financial loss or agency liability;
- Harm to agency program or public interest;
- Personal safety;
- Civil or criminal violation; and
- Unauthorized release of sensitive information.

For each risk description formulated, analyze the potential impact of each risk to the CMS business mission. A listing of sample business impacts is provided in Table 3: Sample Risk Descriptions, Business Impacts, and Existing Controls. Complete the field labeled "Business Impact" in the "Risk and Safeguards Table" with the results of this step.

4.3.6 IDENTIFY EXISTING CONTROLS

Identify existing controls that reduce (1) the likelihood or probability of a threat occurring, and / or business rules that mitigate the impact resulting from threat occurrence and/or (2) the likelihood or probability of a threat exploiting identified system vulnerability, and/or (3) the magnitude of impact of the exploited vulnerability on the system. Existing controls may be management, operational, and/or technical controls depending on the identified threat/vulnerability pair and the risk to the system. A listing of sample existing controls is provided in Table 3, Sample Risk Descriptions, Business Impacts, and Existing Controls.

Table 3: Sample Risk Descriptions, Business Impacts, and Existing Controls

Sample Items	Description
Example	1
Business Function:	Payroll.
Threat:	Supporting business process is not available.
Risk Description:	If the employee time-sheet submission function is unavailable, the payroll function cannot be completed because there is no basis from which to measure employee compensation.
Business Impact:	Employees may not be issued paychecks on time, and employee morale and productivity may suffer.
Existing Controls:	Business rules are established that enable employees to submit timesheets manually to management. Employee payroll processing would be made without the actual time and attendance information. However, these could be tracked manually and adjustments made once these applications were fully restored.
Example	2
Business Function:	Human Resources (HR).
Threat:	HR database is not available.
Risk Description:	If the HR database is not available, no employee information including performance reviews, disciplinary documentation, and achievement memos can be maintained.

Sample Items	Description
Business Impact:	Employee disciplinary documentation may not be issued on a timely basis resulting in a delayed termination of an undesirable employee.
Existing Controls:	Business Rules allow for manual preparation and storage of essential HR documents until the database becomes available.
Example	3
Business Function:	Medicare Claims Payment.
Threat:	Information resource erroneous.
Risk Description:	Given an error in an information resource, an incorrect Medicare payment will be issued.
Business Impact:	CMS or its providers may incur financial loss.
Existing Controls:	Business Rules require that Medicare claims payment data be reviewed and validated prior to issuing payment.
Example	4
Business Function:	Accounting.
Threat:	Person preparing the check is same as the person authorizing the check.
Risk Description:	An incorrect Medicare payment could be issued.
Business Impact:	CMS or its providers may incur financial loss.
Existing Controls:	Business Rule requires two different signatures on a check through separation of duties.

Complete the field labeled “Existing Controls” in the “Risk and Safeguards Table” with the result of this step.

4.3.7 DETERMINE THE LIKELIHOOD OF OCCURRENCE

Determine the likelihood that a threat will materialize or that a threat will exploit any vulnerability. The likelihood is an estimate of the frequency or the probability of such an event. The likelihood of occurrence is based on a number of factors that include the following:

1. Nature of the business function and the type of information and resources supporting the business processes;
2. The business rules, system architecture, system environment, information system access, and existing controls;
3. The presence, motivation, tenacity, strength, and nature of the threat;
4. The presence of vulnerabilities; and
5. The effectiveness of existing controls.

Refer to the information provided in Table 4, Likelihood of Occurrence Levels for guidelines to determine the likelihood of threat occurrence. Complete the column labeled ”Likelihood of Occurrence“ in Table 7, Risks and Safeguard table with the results of this step.

Table 4: Likelihood of Occurrence Levels

Likelihood	Description
Negligible	Unlikely to occur

Very Low	Likely to occur two / three times every five years
Low	Likely to occur once every year or less
Moderate	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

4.3.8 DETERMINE THE IMPACT SEVERITY

Determine the magnitude or severity of impact on (1) the business function if the existing controls and business rules are applied and the threat still materializes and (2) the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. Determine the severity of impact for each threat or threat/vulnerability pair by evaluating the potential loss in each of the areas of CIA based on (1) the business function criticality and sensitivity levels and (2) the system's information security level as explained in the *CMS System Security Level by Information Type* document. The impact can be measured by a partial or full loss of the business function, the inability to meet/complete a CMS business mission, monetary losses, loss of public confidence, unauthorized disclosure of data, loss of system functionality, and/or degradation of system response time. Refer to Table 5, Impact Severity Levels, for guidelines on impact severity levels.

Table 5: Impact Severity Levels

Impact Severity	Description
Insignificant	• Will have almost no impact if the threat occurs/vulnerability is exploited. • Will result in minimal loss of functional integrity. • Requires little or no recovery cost.
Minor	• Will have some minor effect on the business function/system. • May cause minor financial loss, but will not result in negative publicity or political damage. • Will require only minimal effort to complete corrective actions and continue or resume operations. • Will require minimal effort to repair or reconfigure the system.
Significant	• Will result in some tangible harm, albeit negligible, and perhaps only realized by a few individuals or agencies. • May cause political embarrassment, negative publicity, and moderate financial loss. • Will require a moderate expenditure of resources to repair.
Damaging	• May cause damage to the reputation of system management, CMS, and/or notable loss of confidence in the ability for CMS to complete its stated business mission, system resources and services. • May result in legal liability, and will require significant expenditure of resources to repair or to complete corrective actions and restore operations.

Impact Severity	Description
Serious	• May cause considerable disruption in the business function, system outage and/or loss of customer or business partner confidence. • May result in compromise of large amount of Government information or services, a substantial financial loss, and the failure to deliver CMS public programs and services.
Critical	• May cause an extended disruption in the business function, system extended outage. • May require recovery in an alternate site environment or hot site environment. • May result in full compromise of CMS' ability to provide public programs and services, and ability to complete the stated business mission.

4.3.9 DETERMINE THE RISK LEVEL

The risk can be expressed in terms of the likelihood of threat occurrence / threat exploiting vulnerability and the severity of impact. Mathematically, the Risk Level is equal to the Likelihood of Occurrence multiplied by Impact Severity as follows:

Risk Level = Likelihood of Occurrence X Impact Severity

The Business Owner may increase the risk to a higher level depending on the system security level and the level of compromise if a threat is realized. However, the Business Owner cannot lower the risk level unless the likelihood of occurrence and severity of impact are also changed. Refer to Table 6, Risk Levels, to determine the level of risk.

Table 6: Risk Levels

Likelihood of Occurrence	Impact Severity **Insignificant**	Impact Severity **Minor**	Impact Severity **Significant**	Impact Severity **Damaging**	Impact Severity **Serious**	Impact Severity **Critical**
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Moderate	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

Risk Determination Process Milestones:

- Complete the Risk Determination items within the Risks and Safeguard Table. Refer to Appendix A for instructions on how to complete the table.

4.4. SAFEGUARD DETERMINATION PROCESS

The Safeguard Determination Process is the third process of the IS RA process. The Safeguard Determination process requires the identification of additional controls, safeguards or corrective actions to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability pair identified during Risk Determination, resulting in moderate or high risk levels.

Controls/safeguards for threat/vulnerability pairs with low risk level do not need to be identified, as the goal of this step is to reduce the risk level to low. The recommended safeguard should aim to reduce the risk level for business and system risks. The residual risk level is determined assuming full implementation of the recommended controls/safeguards. It should also reduce the risk level for both business and system risks. Safeguard Determination comprises four (4) steps and uses the following fields within Table 7, Risks (Business and System) and Safeguards to record the identification of new security measures and address the level of risk already assessed for the threat/vulnerability pair:

- **Recommended Safeguards Descriptions –** Identify the controls/safeguards to reduce the risk level of an identified threat / vulnerability pair, if the risk level is moderate or high.
- **Residual Likelihood of Occurrence –** Determine the residual likelihood of occurrence of the threat if the recommended safeguard is implemented.
- **Residual Impact Severity –** Determine the residual impact severity of the exploited vulnerability once the recommended safeguard is implemented.
- **Residual Risk Level –** Determine the residual risk level for the system.
  A sample of risks and safeguards is provided in Table 7, Risks and Safeguards (Sample).

TASK 3: UPDATE THE RISKS AND SAFEGUARDS

The Business Owner shall ensure that the following activities take place during this task:

- Recommended Safeguard(s) Descriptions are developed for each threat/vulnerability pair;
- The residual likelihood of occurrence is updated;
- The residual impact severity is updated; and
- The residual risk level is determined.

Task 3 Activities:
Update the Risks and Safeguards Table for Business and System Risks to reflect:

- Recommended Safeguard(s) Descriptions;
- Residual Likelihood of Occurrence;
- Residual Impact Severity; and
- Residual Risk Level.

Table 7: Risks and Safeguards (Sample)

Risks and Safeguards	Response Data
Item No.:	MCP3
Business Function:	Medicare Claims Processing
Threat Name:	Information resource erroneous
Risk Level:	Moderate

Risks and Safeguards	Response Data
Vulnerability Name:	N.A. (not a system risk)
Risk Description:	Given an error in an information resource, an incorrect Medicare payment will be issued.
Business Impact:	CMS may incur a financial loss.
Existing Controls:	Business rules require Medicare claims payment data be reviewed and validated prior to processing.
Likelihood of Occurrence:	Medium
Impact Severity:	Significant
Risk Level:	Moderate
Recommended Safeguard Description:	An automated control validates the consistency and accuracy of Medicare claims payment data before payments are issued.
Residual Likelihood of Occurrence:	Low
Residual Impact Severity:	Minor
Residual Risk Level:	Low
Implementation Priority:	1
Implementation Rationale:	This risk has been granted a high priority as the occurrence of an error will result in financial loss to CMS and absence of a control could result in fraudulent activity being performed by claimants.

The objective of this task is to update the Risks and Safeguards Table. To accomplish this, the Business Owner and/or author must update the Risks and Safeguards by performing the following:

- Describe the recommended safeguard(s);
- Determine the residual likelihood of occurrence;
- Determine the residual impact severity; and
- Determine the residual risk level.

4.4.1 DESCRIBE THE RECOMMENDED SAFEGUARDS

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination Process. Recommended safeguards will address the security category CIA identified during the risk analysis process that may be compromised by the exploited vulnerability. The purpose of the recommended safeguard is to reduce or minimize the level of risk. When identifying a safeguard, consider the following:

- Security area where the safeguard belongs, such as management, operational, and technical;
- Method the safeguard employs to reduce the likelihood of a threat materializing or presenting an opportunity for the threat to exploit the vulnerability;
- Effectiveness of the proposed safeguard to mitigate the risk level; and
- Policy and architectural parameters required for implementation in the CMS environment.

To determine safeguards for authentication risks resulting from electronic transactions, Business Owners must consider the entire E-authentication process. The Business Owner must determine the requirements for each step in the E-authentication/authorization process. See Appendix B, E-Authentication Assurance Levels.

4.4.2 DETERMINE THE RESIDUAL LIKELIHOOD OF OCCURRENCE

The Residual Likelihood of Occurrence represents the Likelihood of Occurrence once the Recommended Safeguard(s) has been implemented.

4.4.3 DETERMINE THE RESIDUAL IMPACT SEVERITY

The Residual Impact Severity represents the Impact Severity once the Recommended Safeguard(s) has been implemented.

4.4.4 DETERMINE THE RESIDUAL RISK LEVEL

Determine the residual risk level for the threat/vulnerability pair and its associated risk once the recommended safeguard(s) is implemented. The residual risk level is determined by examining the likelihood of occurrence of the threat materializing or exploiting the vulnerability and the impact severity factors in categories of CIA (see "Risk Level"). Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard should reduce the risk level to Low or completely mitigate the risk. If special conditions exist, describe them with a narrative below the risks (Business and System) safeguards description.

Safeguard Determination Process Milestones:
Complete Safeguard Determination and Residual Risk Level within the Risks (Business and System) and Safeguards Tables.

4.5. SAFEGUARD IMPLEMENTATION PROCESS

The Safeguard Implementation Process is the fourth and final process of the IS RA Process. The Safeguard Implementation Process consists of two processes that address the following:

- Assign a priority to the safeguards; and
- Provide the rationale for the prioritization of the safeguards.

TASK 4: DETERMINE IMPLEMENTATION PRIORITY AND RATIONALE

The Business Owner shall ensure that the Risks and Safeguards Table is updated once the implementation priority and rationale for the ranking have been completed.

Task 4 Activities:
1. Determine the implementation priority.
2. Describe the implementation rationale.
3. Update the Risks and Safeguards Table.

4.5.1 DETERMINE THE IMPLEMENTATION PRIORITY

Once the risks have been evaluated in terms of likelihood of occurrence and impact severity, and when the recommended safeguards have been reviewed, it is then meaningful to rank the risks from highest to lowest in order to assign priorities. The task of prioritizing the risks is conducted at the Business Owner level to ensure that all political, business, and programmatic factors are weighted appropriately in the priority assessment. Management must exercise judgment to assign resources for risk management efforts in response to the priorities identified. The ranked risks are reviewed in terms of combined likelihood and impact severity, and in terms of business level concerns with missions, functions, business objectives, and political concerns.

4.5.2 DESCRIBE THE IMPLEMENTATION RATIONALE

The Business Owner should analyze the feasibility and effectiveness of recommended safeguards. It is not always practical to implement all the solutions because of technical, physical, time, or financial constraints. A cost-benefit analysis should be prepared describing costs and benefits of implementing or not implementing recommended safeguards. The Business Owner should provide a summarized approach for control implementation including all resources, which can be used by the CIO in the C&A process.

Recommended Safeguard Implementation Process Milestones:
Completed Risks and Safeguards Table with the implementation priority and rationale.

APPENDIX A IS RA TEMPLATE INSTRUCTIONS

This appendix of the procedures provides detailed instructions for completing an IS RA. The Business Owner shall follow these instructions in completing the IS RA Template. The Business Owner shall perform system identification by documenting the system name, related information, and the responsible organization. The system must be categorized as a GSS, GSS sub-system, MA or an individual application with an MA.

REVIEW LOG

Update the IS RA review log with the following:

- Date the IS RA was reviewed;
- Staff name of the reviewer; and
- Organization of the reviewer.

INTRODUCTION

The IS RA contains a list of threats and vulnerabilities, an evaluation of current security controls, their resulting risk levels, and any recommended safeguards to reduce risk exposure. The IS RA also supports risk management through the evaluation of risk impact upon the enterprise security model.

SYSTEM NAME/TITLE

Provide the system identifier which include the Official name and/or title of system, including acronym, and system of records (SOR) number, the Financial Management Investment Board (FMIB) number and the system type.

Instruction:
Provide the following:

- Official name and/or title of system,
- System acronym,
- SOR number,
- FMIB number, and
- Type of system.

SOR Number
SOR number can be obtained from the CMS Privacy Officer and must remain the same throughout the life of the system and be retained in audit logs related to system use. Assignment of a SOR number supports CMS' ability to collect CMS information and security metrics specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance.

FMIB Number
During the "Framework" Implementation Phase, the investment is reviewed by the Information Technology Investment Review Board (ITIRB)/FMIB. Approved investments are subsequently assigned an FMIB number. The FMIB number facilitates complete traceability to ensure continued visibility of the investment assessed by compliance with

established scope, budget, schedule, and performance measures.

System Type
For CMS systems, indicate whether the system is an MA, MA individual application, GSS, or GSS sub-system. If the system contains minor applications, describe them in the General Description/Purpose section of the plan.

Note: For non-CMS systems/applications, more than one system type can be indicated. For any MA or MA individual application supported by a GSS which is not one of the CMS System Families, the Business Owner has the option of combining the GSS and MA (or MA individual application) IS RA requirements into one IS RA and the GSS and MA (or MA individual application) SSP requirements into one SSP. This same option is available to the External Business Partners (e.g., Fiscal Intermediaries, Carriers, etc.). Check the appropriate boxes.

Determine if the System is a GSS or a GSS sub-system / MA or MA individual application
The Business Owner works with the OIS CISO to determine if the system is either a GSS or a MA and what FISMA system family it will be categorized. Once the Business Owner has obtained this designation, the identification of the System Security Level by Information Type is determined. Upon establishing the level, the Business Owner will review the CMS PISP and CMS IS ARS for the level of controls that must be employed in the system. An IS RA must be conducted for each GSS, GSS sub-system (if applicable), MA and MA individual application.

A GSS is a grouping of systems that consist of interconnected information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and provides general support for a variety of users and/or applications. As a rule of thumb, a GSS is a physical platform and infrastructure upon which applications run (e.g., mainframe systems, web servers, communications equipment, etc.). All CMS internal system infrastructure is accountable within one of six GSS SSPs (i.e., CMS Data Center, Regional Offices, Web Hosting, Medicare Data Communications Network (MDCN), Quality Net, and Medicare Data Centers).

A GSS sub-system is a logical grouping of systems that support a single GSS and will require the implementation of both an IS RA and SSP to provide comprehensive security assessment and planning.

An MA is a grouping of CMS application systems that support clearly defined business functions for which there are readily identifiable security considerations and needs (e.g., Administrative Finance Systems, Customer Service Systems, Managed Care Systems, Medicare Beneficiary Enrollment Systems, etc.). A MA is usually comprised of multiple application systems and occasionally might have hardware, software, and telecommunication components. These components can be a single software application or a combination of hardware/software focused on supporting a specific business-related

function. MA SSPs only need to document the security controls specific to the MA and how, if applicable, their system adds to or deviates from the controls supported by the higher-level GSS and/or Master Plan.

An MA individual application is a logical identification of a single application that will require the implementation of both an IS RA and SSP to provide comprehensive security assessment and planning.

RESPONSIBLE ORGANIZATION

Provide the contact information for the **CMS** organization responsible for the system. A designated responsible organization must be identified in the IS RA for each system. The organization is responsible for coordinating "Framework" activities specific to the system.

Instruction:
Identify the responsible organization for the system.

The IS RA should include the following responsible organization contact information:

- Name of Organization;
- Address;
- City, State, Zip;
- Contract Number; and
- Contract Name.

In addition to the CMS responsible organization, contractors, and other CMS partners, can document their company specific information in another table that must be added below the table that documents the CMS information. However, this is optional.

DESIGNATED CONTACTS

Indicate the names of other key contact personnel who can address inquiries regarding system characteristics and operation. Required contacts include, but are not limited to, Business Owner, System Developer/Maintainer, and RA author. The IS RA should include the following contact information for each of the designated contacts:

Instruction:
Identify additional personnel that can address system related inquiries. Provide contact information for each.

- Name (Business Owner);
- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail;
- Phone; and
- Contractor contact information (if applicable).

ASSIGNMENT OF SECURITY RESPONSIBILITY

This section requires two (2) different security contacts - one (1) primary security contact and one (1) different emergency contact. A CMS individual responsible for security shall be identified as the primary contact. The emergency contact should know how to contact the primary contact or his/her supervisor. Emergency contact does not have to be a technical person. If a system is housed or hosted outside of the CMS Data Center facilities, an individual responsible for security and/or a component ISSO contact shall be provided for the contractor or external business partner hosting the system.

Instruction:
Identify two (2) different security contacts.

The assignment of security responsibility shall include the contacts following information:

- Name;
- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail; and
- Phone number
- Emergency Contact (name, phone & email).

SYSTEM OPERATIONAL STATUS

Annotate weather the GSS, GSS subcomponent, MA or individual MA is either new, operational, or undergoing a major modification

Instruction:
Indicate (only one) the system operational status.

DESCRIPTION OF THE BUSINESS PROCESS

Provide a brief description, of the business process and purpose of the system e.g., financial management, network support, business data analysis, research, or procurement. The Business Owner or author shall:

- Indicate the location of the system (external, internal). This high-level description shall include the street address and other information pertaining to the location of the system;

Instruction:
Provide brief descriptions regarding the various business processes.

- Describe the business function for each system;
- Describe the underlying business processes and resources that support each business function. This may include the required inputs (business functions/ processes that feed this function), processing functions (calculations, etc), organizational/personnel roles and responsibilities, and expected outputs/products (that may "feed" other business functions/processes;
- Describe how information flows through and is processed by the system, beginning with system input through system output. Further describe how the data/information is handled by the system (e.g., is data read, stored, purged, etc?);
- Indicate the organizations (i.e., internal & external) that will comprise the user community. Include type of data and processing that will be provided by users, if any; and
- Describe the users' level of access to system related data (e.g., read-only, alter, etc), system related facilities, and information technology resources.

If the system is a GSS, list all applications supported by the GSS. Specify if the application is an MA and include unique name/identifiers, where applicable. Describe each application's function and the information processed.

DESCRIPTION OF OPERATIONAL/SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

***Note: This section differs from the previous section in that it addresses the technical aspects of the system.**

Operational Information

Describe (at a high level) the anticipated technical environment and user community necessary to support the system and business functions. Include:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Be sure to indicate, the physical location of the business processes and technology that will support the system.

System Information

Provide a brief general description of the technical aspects of the system. Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc.

Attach the network connectivity diagram, which shall address the system components' connection, and the security devices, which 1) protect the system and 2) monitor system access and system activity. For systems that have more than one server of the same type, only include one in the diagram; however state the accurate count of the servers in the supporting text description. Be sure to provide an opening sentence(s) prior to the diagram. Following the diagram, include text that will explain system components and function. Be sure to number system components in the diagrams so as to correlate the information presented.

Instruction:

Provide operational related information regarding:

- Communications requirements,
- User-interface expectations, and
- Network connectivity requirements.

Provide system related information regarding:

- System Environment;
- Architecture & Topology;
- Boundary Issues;
- Primary Platforms & Security Software;
- System Interconnectivity Interfaces, Web protocols, and computing environments; and
- Special Security Concerns

"N.A" can be specified as appropriate.

Attach the network connectivity diagram

System Environment

Provide a description of the system environment.

- Is the system owned or leased?
- Is the system operated by the Government or by a service support contractor?
- If the system is maintained or "run" by a contractor, describe (comprehensively) how the system is managed.
- Document the hours of operation; e.g., 24x7, M-F 7:30 am – 5:00 pm.
- Document the approximate total number of user accounts and unique user types (i.e., researchers, programmers, administrative support, etc.).
- Identify the critical processing periods (e.g., payroll processing.).
- If system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies.).
- List all applications supported by the system including the applications' functions and information processed.
- Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.
- Describe the information/data stores within the system and security controls for such data.
- Describe how both the system's information and operation serve as an asset to CMS.
- Describe the purpose and capabilities of the information system.
- Describe the functional requirements of the information system. For instance:
  - Are protection mechanisms (i.e., firewalls) required?
  - Are support components such as web servers, and e-mail required?
  - What types of access mechanisms (i.e., telecommuting, broadband communications) are required.
  - Are "plug-in" methods (Mobile code; Active-X, Javascript) required?
  - What operating system standards, if any, are required?

Architecture and Topology

Describe the architecture of the information system. If this is documented in another master or subordinate system plan, reference it by unique identifier and plan name.

- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and how this addresses security.

Boundary Issues

Provide a detailed description of the system's boundaries and technical components.

- Describe the boundary of the information system for security accreditation.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network topology.

- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.
- Following the logical diagram, describe the information flow or processes within the system to access the data/information.

Primary Platforms and Security Software

Describe the primary computing platform(s) used and describe the principal system components, including hardware, firmware, software, wireless, and communications resources. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). This will include vendors and versions.

- Include information concerning a system's hardware and platform(s).
- Detailed hardware equipment information, such as server names, shall be listed and attached to the documentation.
- Describe any security software protecting the system and information.
- Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the security features that are available in the software.

Interconnectivity Interfaces, Web Protocols, and distributed & collaborative computing environments

Describe the Web protocols and distributed, collaborative computing environments (e.g., processes and applications).

- Describe the connectivity between modules within the scope of this system.
- For systems that interface with the Internet, describe how the architecture does/does not match the CMS Internet Platform Architecture.
- For any system that allows individual web-based access (Internet, Intranet or Extranet) to conduct transactions the following information should be provided:
  - The Uniform Resource Locator (URL) for the web-based transaction;
  - E-authentication architecture implemented;
  - E-authentication interoperable product used;
  - Other authentication products used;
  - Number of electronic logins per year;
  - Number of registered users (Government to Government);
  - Number of registered users (Government to Business);
  - Number of registered users (Government to Citizen);
  - Number of registered internal users; and
  - Description of customer groups being authenticated, e.g., Business Partners, Medicare Service Providers, Beneficiaries, etc.

Special Security Concerns

Include any environmental or technical factors that raise special security concerns, such as:

- Indicate the physical location of the information system;

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is implemented rapidly;
- The software resides on an open network used by the public or with overseas access; and
- The application is processed at a facility outside of CMS control.

SYSTEM INTERCONNECTION/INFORMATION SHARING

System interconnection is the direct connection of two or more IT systems for sharing information resources. It is important that Business Owners, and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential in selecting the appropriate controls required to mitigate those vulnerabilities.

A CMS Interconnection Security Agreement (ISA) or CMS Memorandum of Understanding (MOU) is required between systems, which both share data, and are owned or operated by different organizations. If the system interconnection/information sharing is between two or more CMS systems located internal to the CMS secure network infrastructure, the Business Owner shall utilize and follow the CMS MOU procedures. If the system interconnection/information sharing is between a CMS system and a system located external to the CMS secure network infrastructure, the Business Owner shall utilize and follow the CMS IS RA procedure.

SYSTEM SECURITY LEVEL

Identify the system security level. Each system identified in the CMS system inventory must be categorized using CMS System Security Level by Information Type, which can be found at the CMS IS web site, http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf .

If multiple categories apply, the highest-level category is defined as the Sensitivity level for the system.

Instruction:

- Categorize the system based on the *CMS System Security Level by Information Type* in the table.
- Describe in general terms the information handled by the system and the protective measures.

E-AUTHENTICATION ASSURANCE LEVEL

Indicate the appropriate system's/application's ability to provide web-based access to individuals for the purpose of conducting transactions. If web-based transactions are permitted, and RACF/Top Secret/Active Directory (or equivalent) is used to authenticate individuals, check the appropriate box.

Use the E-authentication Workbook to establish the level of security required for the

system. The Workbook addresses all four (4) levels of assurance for E-authentication and has been developed into two aspects "Registration and Identify Proofing" and "Authentication Mechanism Requirements" that correspond to the four system assurance levels.

RISKS AND SAFEGUARDS TABLE

Use the Business Risk and System Risk tables to provide the following information:

- Item Number (System Acronym + sequential item #; i.e. EDB - 1);
- Business Function;
- Risk Level (current, unmitigated risk level);
- Threat Name;
- Vulnerability Name;
- Risk Description;
- Business Impact;
- Existing Controls;
- Likelihood of Occurrence;
- Impact Severity;
- Risk Level;
- Recommended Safeguard Description;
- Residual Likelihood of Occurrence;
- Residual Impact Severity, and Residual Risk Level;
- Implementation Priority; and
- Implementation Rationale.

Threats and vulnerabilities shall be treated as a pair. Each threat/vulnerability pair shall be addressed individually to simplify identification of existing controls for the threat / vulnerability pair and for the determination of the risk level. Further, threat/vulnerability pairs may be grouped by category (environmental, physical, human, natural, and technical) for clarity.

Item Number

The Item Number (Item No.) designated in the upper left corner is for reference purposes only. The Item Number will consist of the system / sub-system acronym in front of a number. Numbers will be assigned in numerical order as rows are added to the table for different threat/vulnerability pairs (e.g., the first threat/vulnerability pair for Application A will result in Item No. of A-1).

Business Function

Identify and define the business function that will be reviewed in the context of the risk.

Threat Name

Identify threats that could have the ability to exploit system vulnerabilities.

Vulnerability Name

Identify vulnerabilities associated with each threat to produce a threat/vulnerability pair.

Risk Description

Describe how the vulnerability when exploited by the threat creates a risk in the system in terms of CIA elements that may result in a compromise of the system and the data it handles.

Business Impact

Determine the impact to the business function that could occur due to the compromise of a system.

Existing Controls

Identify existing controls that reduce: (1) the likelihood or probability of a threat exploiting identified system vulnerability, and/or (2) the magnitude of impact of the exploited vulnerability on the system.

Likelihood of Occurrence

Determine the likelihood that a threat will exploit any vulnerability. The likelihood is an estimate of the frequency or the probability of such an event.

Impact Severity

Determine the magnitude or severity of impact on the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. Determine the severity of impact for each threat/vulnerability pair by evaluating the potential loss in each security category CIA based on the system's information security level as explained in the *CMS System Security Level by Information Type* document. The impact can be measured by loss of system functionality, degradation of system response time, or inability to meet a CMS business mission, dollar losses, loss of public confidence, or unauthorized disclosure of data.

Risk Level

The risk can be expressed in terms of the likelihood of threat occurrence and the severity of business impact. Mathematically, the Risk Level is equal to the Likelihood of Occurrence multiplied by the Impact Severity in the business function's CIA as follows:

Risk Level = Likelihood of Occurrence X Impact Severity

Recommended Safeguard Description

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination Process. Recommended safeguards will address the security category CIA identified during the risk analysis process that may be

compromised by the exploited vulnerability. If more than one safeguard is identified for the same threat/vulnerability pair, list them in this column in separate rows and continue with the analysis steps. The residual risk level must be evaluated during this process of the assessment and may be further evaluated in RM activities.

Residual Likelihood of Occurrence

The Residual Likelihood of Occurrence represents the Likelihood of Occurrence once the Recommended Safeguard has been implemented. As such, follow the instructions described in the Likelihood of Occurrence, while assuming full implementation of the recommended safeguard.

Residual Impact Severity

The Residual Impact Severity represents the Impact Severity once the Recommended Safeguard has been implemented. As such, follow the instructions described in the Impact Severity, while assuming full implementation of the recommended safeguard.

Residual Risk Level

Determine the residual risk level for the threat/vulnerability pair and its associated risk once the recommended safeguard is implemented. The residual risk level is determined by examining the likelihood of occurrence of the threat exploiting the vulnerability and the impact severity factors in categories of CIA. As such, follow the instructions described in the Risk Level to determine the residual risk level once the recommended safeguard is fully implemented. Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard should reduce the risk level to Low. If special conditions exist, describe them with a narrative below the table.

Implementation Priority

Once the risks have been evaluated in terms of likelihood of occurrence and impact severity, and when the recommended safeguards have been reviewed, it is then meaningful to rank the risks from highest to lowest in order to assign priorities.

Implementation Rationale

The implementation rationale provides the explanation for order, sequence, and justification for which recommended safeguard(s) will be implemented and when.

APPENDIX B E-AUTHENTICATION ASSURANCE LEVELS

E-authentication is the process of establishing reasonable confidence in user identities presented electronically to an information system to conduct transactions. Individual authentication is the process of establishing an understood level of confidence that an identifier, for the purpose of conducting transactions, refers to a specific individual. E-authentication assurance levels are based upon the degree of confidence in the approval process used to establish the identity of the individual web-user to whom the credential was issued, and the degree of confidence that the individual who uses the credential is the individual web-user to whom the credential was issued. Each transaction can have an assurance level associated with it, depending upon the type of transaction. To assign the appropriate assurance level for E-authentication, the Business Owner must identify the appropriate potential impact levels by authentication error category for each transaction type, as they are described in the following sub-sections.

DETERMINE POTENTIAL IMPACT LEVELS BY AUTHENTICATION ERROR CATEGORY

Assurance levels for transaction types are determined by assessing the potential impact, of several authentication error categories, using the potential impact values described in Federal Information Processing Standard (FIPS) 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* Table 8 lists the categories of authentication errors and defines the levels of potential impacts for each error. For each transaction type, assign appropriate levels for the potential impact by Authentication Error Category, as listed in Table 8.

Table 8: Potential Impact Categories and Level Definitions

Authentication Error Category	Low Level of Potential Impact	Moderate Level of Potential Impact	High Level of Potential Impact
Inconvenience, distress or damage to standing or reputation	At worst, limited, short-term inconvenience, distress or embarrassment to any party.	At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
Financial loss or agency liability	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	At worst, a serious Unrecoverable financial loss to any party, or a serious agency liability.	Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.
Harm to agency programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. (e.g. (i) mission	At worst, a serious adverse effect on organizational operations or assets, or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. (e.g. (i) severe mission

Authentication Error Category	Low Level of Potential Impact	Moderate Level of Potential Impact	High Level of Potential Impact
	capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	(e.g. (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	capability degradation or loss to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Unauthorized release of sensitive information	At worst, a limited release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact.	At worst, a release of personal, U.S. Government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact.	A release of personal, U.S. government sensitive or Commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact.
Personal Safety	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
Civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

ASSIGN E-AUTHENTICATION ASSURANCE LEVEL

Office of Management and Budget (OMB) M-04-04 E-Authentication Guidance, describes four assurance levels for electronic transactions. These levels represent ranges of confidence in an electronic identity presented to an agency by means of a credential. The levels are numbered from one (1) to four (4) with 1 being minimal and 4 being the highest level of identity assurance.

In assigning the assurance level, the Business Owner must consider all the direct and indirect consequences as presented in the definitions of the levels. The Business Owner needs to consider the terms “minimal”, “minor”, “significant”, or “considerable” in the context of the users likely to be affected. To determine the required assurance level, identify risks inherent in the transaction process regardless of its authentication technology. Associate the authentication error category outcomes to the assurance level for each threat, choosing the lowest level of assurance that will cover all identified potential impacts. Thus, if six categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 assurance.

The four assurance levels are:

Level 1: Minimal Assurance – Level 1, little or no confidence is placed in the asserted electronic identity of the user. In particular, an authentication threat of user's identity at level 1 would result in the following:

- Minimal inconvenience to anyone;
- No financial loss to anyone;
- Minimal distress being caused to anyone;
- No risks or harm to CMS program or other public interest;
- No release of personal data, CMS sensitive data, or commercially sensitive data to unauthorized parties; and
- No risk to anyone's personal safety.

Level 2: Low Assurance – Level 2 is appropriate for transactions in which some confidence in the asserted electronic identity of the user is sufficient. In particular, an authentication threat of user's identity at level 2 might result in at most, the following:

- Minor inconvenience to anyone;
- Minor financial loss to anyone;
- Minor distress being caused to anyone;
- Minor risks or harm to a CMS program or other public interest;
- A Minor release of personal data, or commercially sensitive data to unauthorized parties;
- No release of CMS sensitive data to unauthorized parties; and
- No risk to anyone's personal safety.

Level 3: Substantial Assurance – Level 3 is appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the user. In particular, an authentication threat of user's identity at level 3 might result in the following:

- Significant inconvenience to anyone;
- Significant financial loss to anyone;
- Significant distress being caused to anyone;
- Significant harm to CMS program or other public interest;
- A significant release of personal data, CMS sensitive data, or commercially sensitive data to unauthorized parties; and
- No risk to anyone's personal safety.

Level 4: High Assurance – Level 4 is appropriate for transactions that are official in nature, and for which there is a need for very high confidence in the asserted electronic identity of the user. In particular, an authentication threat of user's identity at level 4 might result in the following:

- Considerable inconvenience to anyone;
- Considerable financial loss to anyone;
- Considerable distress being caused to anyone;

- Considerable harm to a CMS program or other public interest;
- A damaging release of extensive personal data, CMS sensitive data, or commercially sensitive data to unauthorized parties; and
- A risk to anyone's personal safety.

Utilize Table 9 to determine the level of E-authentication assurance for each transaction type. Using the level of impact, assign the assurance level per authentication error category. In some cases (as shown in Table 9), impact may correspond to multiple assurance levels. In such cases, use the system/application context to determine the appropriate assurance level.

Table 9: Assurance Level by Authentication Error Category Impact

Potential Impact Categories for Authentication Error	1	2	3	4
A - Inconvenience, distress or damage to standing or reputation	**Low**	**Mod**	**Mod**	**High**
B - Financial loss or agency liability	**Low**	**Mod**	**Mod**	**High**
C - Harm to agency programs or public interests	**N/A**	**Low**	**Mod**	**High**
D - Unauthorized release of sensitive information	**N/A**	**Low**	**Mod**	**High**
E - Personal Safety	**N/A**	**N/A**	**Low**	**Mod High**
F - Civil or criminal violations	**N/A**	**Low**	**Mod**	**High**

The Assurance Level impact is defined in columns two through five.

DOCUMENT TRANSACTION ASSURANCE LEVEL

Complete the columns labeled under "Transaction Assurance Level" in Table 10 with the determined assurance level, corresponding to the category letter, as a result of Table 9, Assign E-authentication assurance level, for each transaction type. Document the highest assurance level for each transaction type in the "Overall" column.

Table 10: Transaction Type Assurance Level Worksheet (not part of the template)

Transaction Type	A	B	C	D	E	F	Overall

The Transaction Assurance Level are defined in columns A through F.

DOCUMENT SYSTEM/APPLICATION ASSURANCE LEVEL

To determine the overall E-authentication Assurance Level required for the system/application, take the highest level of assurance from Table 10, "Transaction Type Assurance Level Worksheet", from the column labeled "Overall". Complete the column labeled "Assurance Level" in Table 11 with the overall E-authentication assurance level for the system/application.

Table 11: E-authentication Assurance Level

E-authentication Assurance Level

To implement controls that meet with the required standards outlined in NIST SP 800-63 "*Recommended Security Controls for Federal Information Systems*", refer to the CMS IS ARS for guidance.

APPENDIX C IS RA ACTIVITIES CHECKLIST

System Name _____

Business Owner _____

STEPS	DATE COMPLETED	COMPLETED BY
BUSINESS FUNCTION/SYSTEM DOCUMENTATION PROCESS		
Task 1-Initation of the IS RA		
1. Assess the information processed by the system		
2. Document the business processes and technical environment		
3. Establish system security level by information type		
4. Determine E-authentication Assurance Level		
5. Complete the System Security Plan Workbook		
6. Define technical requirements and operational practices		
RISK DETERMINATION PROCESS		
Task 2-Complete the risk determination items within the risks and safeguards table		
1. Document the business function		
2. Document the threat to the business function/system		
3. Document the vulnerabilities for the system		
4. Provide the risk description, business impact and existing controls		
5. Provide the likelihood of occurrence and impact severity		
6. Calculate the risk level		
SAFEGUARD DETERMINATION PROCESS		
Task 3-Update the risks and safeguards table		
1. Provide the recommended safeguard descriptions		
2. Provide the residual likelihood of occurrence		
3. Provide the residual impact severity		
4. Provide the residual risk level		

STEPS	DATE COMPLETED	COMPLETED BY
SAFEGUARD IMPLEMENTATION PROCESS		
Task 4-Complete the risks and safeguards table		
1. Determine the implementation priority.		
2. Describe the implementation rationale.		
3. Update the Risks and Safeguards Table.		
4. Determine the implementation priority.		

APPENDIX D ACRONYMS

ARS	Acceptable Risk Safeguard
C&A	Certification & Accreditation
CAP	Corrective Action Plan
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
DITPPA	Division of IT Policy, Procedures, & Audits
EASG	Enterprise Architecture & Strategy Group
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FMIB	Financial Management Investment Board
FRAMEWORK	CMS IT Investment Integrated System Development Life Cycle Framework
GSS	General Support System
HR	Human Resources
IRB	Investment Review Board
IS	Information Security
ISA	Interconnection Security Agreement
ISSO/SSO	Information System Security Officer/System Security Officer
IS RA	Information Security Risk Assessment
IT	Information Technology
ITIRB	Information Technology Investment Review Board
IVR	Individual Voice Recognition
MA	Major Application
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PISP	CMS Policy for the Information Security Program
POA&M	Plan of Action & Milestone
RA	Risk Assessment
RAD	Rapid Application Development
RACF	Resource Access Control Facility
RM	Risk Management
SCT	Security Control Testing
SDLC	System Development Life Cycle
SP	Special Publications
SOR	System of Records
SSP	System Security Plan

ST&E	Security Test & Evaluation
URL	Uniform Resource Locator
WAN	Wide Area Network

End of Document