DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Services (OIS)
Systems Security Group (SSG)
Division of Security Policy and Assessments (DSPA)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Risk Assessment Methodology

Version # 2.1
April 22, 2005

Summary of Changes

V2.1

1. Summary of Changes page added
2. Minor formatting changes

V2.0

1. E-Authentication Guidance as required by the
   - Government Paperwork Elimination Act of 1998,
   - OMB M 04-04 E-Authentication Guidance, and
   - NIST SP 800-63, Electronic Authentication Guideline

2. The following sections have been added regarding E-authentication:
   - 1.4 Document E-Authentication Assurance Level
   - 1.4.1 Determine Potential Impact Levels by Authentication Error Category
   - Table 1: Potential Impact Categories and Level Definitions
   - 1.4.2 Assign E-Authentication Assurance Level
   - Table 2: Assurance Level by Authentication Error Category Impact
   - 1.4.3 Document Transaction Assurance Level
   - Table 3: Transaction Type Assurance Level Worksheet
   - 1.4.4 Document System/Application Assurance Level
   - Table 4: E-Authentication Assurance Level

3. The following sections have been added regarding incorporation of Information Security Business Risk Assessments
   - 2.1 Incorporate Risk from IS Business RA
   - 2.1.1 Mapping Business Risks

4. Minor formatting changes

Table of Contents

Overview

The Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Risk Assessment (RA) Methodology presents a systematic approach for the Risk Assessment (RA) process of automated information systems within the CMS environment. This methodology describes the steps to produce an IS RA for systems that are part of a General Support System (GSS), Major Application (MA), individual applications within an MA or sub-systems within a GSS. The IS RA includes a system overview to give a basic understanding of the system and its interconnections, and describes the overall system security level. As part of this approach, the methodology will restate the threats associate to the business functions and address the threats affecting the system's functions which supply the foundation for the IS RA. Additionally, the IS RA provides an evaluation of current security controls to safeguard against the identified threat/vulnerability pairs and the resulting risks levels; and the recommended safeguards to reduce the system's risk exposure with a revised residual risk level once the recommended safeguards are implemented.

The IS RA process is presented in the following five phases:

- System Documentation Phase
- Risk Determination Phase
- Safeguard Determination Phase
- Implementation Phase

The System Documentation phase includes a system overview which describes the system boundaries, a basic synopsis of the system and its interconnections, and describes the overall system security level.

The Risk Determination and Safeguard Determination phases will record the business risks that were identified in the IS Business RA and a list of system threats and vulnerabilities; an evaluation of current security controls to safeguard against the identified threat/vulnerability pairs and the resulting risks levels; and the recommended safeguards to reduce the system's risk exposure with a revised residual risk level once the recommended safeguards are implemented.

The E-authentication Assurance Level Phase is required by the Government Paperwork Elimination Act of 1998 and stipulates that most transactions currently accomplished by filing Government paper forms will be converted to an electronic format. These transactions will require some type of identity verification or authentication before taking place. It is also crucial that these electronic transactions incorporate an appropriate level of security. Agencies providing e-government services need to determine how certain they need to be of the identity of an individual and identify the risk inherent in a particular transaction.

This section provides the system owner with guidance on electronic identity and attributes for authentication (or e-Authentication). e-Authentication can be defined as the process of establishing confidence in both identities and attributes after being electronically presented to an information system. This section provides instruction for implementing e-Authentication processes by:

- Outlining a process for assessing risk,
- Describing four levels of identity assurance, and
- Explaining how to determine the appropriate level of identity assurance.

The Implementation phase of the IS RA process described in this methodology is an integral part of risk management. Risk management also includes prioritization of risks, categorization of recommended safeguards, their feasibility of implementation, and other risk mitigation processes and solutions within the management, operational and technical environment. These risk management activities are beyond the scope of this methodology and are performed as part of the CMS IS Certification and Accreditation (C&A) process as it affects the organization's security posture and management assesses an acceptable level of risk for continuation of operations.

The following appendices are included in the methodology to assist the system owner or IS RA author in the IS RA analysis and provide further clarification and references to complete the IS RA:

Appendix A	Risk Assessment Process Flow - Depicts the IS RA process flow detailed in this methodology for ease of reference
Appendix B	Security in the System Development Life Cycle - Describes information security deliverables and resources as they relate to the System Development Life Cycle and the CMS Integrated IT Investment and System Life Cycle Framework (CMS Framework).
Appendix C	References - Provides additional explanations, examples and locations of useful resources, and tools to aid the IS RA author during the IS RA analysis and report preparation.
Appendix D	CMS Information Security Risk Assessment Template - Facilitates the IS RA documentation, and provides a common and consistent format for the IS RA.

Refer to the *CMS Information Security Terms and Definitions* document for information security terms used throughout this methodology.

Purpose

The *CMS IS RA Methodology* has been developed as a tool to guide system owners and IS RA authors in evaluating and documenting the system's management, operational and technical security environment. This tool describes the steps to produce the IS RA, which is incorporated into the System Security Plan (SSP) and is reviewed during the CMS IS C&A process. The IS RA process supports risk management in the evaluation of the system(s) risk impact upon CMS' enterprise security model. In addition, the threats associated with the business functions will be incorporated into the IS RA process for proper mitigation in the GSS or MA. The IS Business RA process is distinct from the IS RA process. Please refer to the *CMS Information Security Business Risk Assessment Methodology* for more details.

CMS requires each system to have an IS RA in each of the following instances: new system, every third year of an operational system, major system modification(s), increase in security risks/exposure, increase of overall system security level, serious security violation(s) as

described in the *CMS Information Security Incident Handling Procedures* and as a result of adverse security evaluations and/or audits. For a new system or a system undergoing a major modification, an IS RA will be developed as part of the SDLC phases. The IS RA steps are illustrated in Appendix B of this methodology and the IS RA Template is provided in Appendix D.

Risk Assessment Process

To perform the IS RA, the system owner must identify the system's threats and associated vulnerabilities. For each threat/vulnerability pair, the system owner determines the severity of impact upon the system's confidentiality, integrity and availability (CIA), and determines the likelihood of the vulnerability exploit occurring given existing security controls. The product of the likelihood of occurrence and the impact severity results in the risk level for the system based on the exposure to the threat/vulnerability pair.

Once the risk level is determined for each threat/vulnerability pair, safeguards are identified for pairs with moderate or high risk levels. The risk is re-evaluated to determine the remaining risk, or residual risk level, after the recommended safeguard is implemented.

In addition, the IS RA process will determine the required level of assurance for electronic transactions. The IS RA will measure the relative severity of the potential harm to CMS or its users of e-government systems and other transaction participants in the event of an improperly validated or unauthorized authentication. Section 2 provides a profile of consequential risks. The level of confidence required in the asserted electronic identity to engage in a transaction is proportionate to the severity of the likely consequences. Therefore, higher assurance level is required.

1 SYSTEM DOCUMENTATION PHASE

The System Documentation Phase provides background information to describe the system and the data it handles, in support of or in fulfillment of the CMS' business mission. This phase establishes a framework for subsequent IS RA phases.

The system owner must provide system identification to include system description, business function and assets, and system security level determination. For new systems, these are defined when the system is first conceived and developed during the SDLC design and implementation phases of the system. These steps are illustrated in the top section in Appendix A: Risk Assessment Process Flow.

1.1 SYSTEM IDENTIFICATION

Document the system name, other related information, and the responsible organization. The system must be categorized as a GSS, an MA, an individual application system within an MA, or a GSS subsystem according to the *CMS Systems Security Plan Methodology*.

Official System Name		
System Acronym		
System of Records (SOR)		
Financial Management Investment Board (FMIB) Number		
System Type	☐ GSS ☐ GSS sub-system	☐ MA ☐ MA individual application

Name of Organization	
Address	
City, State, Zip	
Contract Number, Contractor contact information (if applicable)	

Identify system contacts information using the template below for system owner/manager, business owner/manager, system maintainer manager and IS RA author. If applicable, provide contractor information, (i.e., contractor name, contract number, contact, e-mail address and phone number, Project Officer/Government Task Leader name, e-mail address and phone number.)

Name of Individual	
Title	
Name of Organization	
Address	
Mail stop	
City, State, Zip	
Email Address	

Phone number	
Contractor contact information (if applicable)	

Identify the individual(s) responsible for security and the component's Information System Security Officer.

Name *(Component ISSO)*	
Title	
Name of Organization	
Address	
Mail stop	
City, State, Zip	
Email Address	
Phone number	
Emergency Contact Information (name, phone and e-mail only)	

1.2 DOCUMENT SYSTEM PURPOSE AND DESCRIPTION (ASSET IDENTIFICATION)

To identify the assets covered by the IS RA, provide a complete and concise description of the function and purpose of the system and the organizational business processes supported, including functions and processing of data. If it is part of a GSS, include a list of all supported applications, as well as functions and information processed.

1.2.1 DOCUMENT SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

Provide a complete and concise technical description of the system. Discuss any environmental factors that raise special security concerns and document the physical location of the system. Provide a network diagram or schematic to help identify, define, and clarify the system boundaries.

1.2.2 DOCUMENT SYSTEM INTERCONNECTION/INFORMATION SHARING

For GSS and GSS sub-systems, depict and describe how the various components and sub-networks are connected and/or interconnected to any other Local Area Network (LAN) or Wide Area Network (WAN). For MAs and their individual applications, provide a description of the system and applications and/or other software interdependencies. Suggestion: For ease and continuity, develop the data flow diagram first and then develop the text to support that diagram.

1.3 DOCUMENT SYSTEM SECURITY LEVEL

Describe and document the information handled by the system and identify the overall system security level as LOW, MODERATE, or HIGH. This element includes a general description of the information, the information sensitivity, and system criticality; which includes requirements for CIA, audit ability and accountability as dictated by *CMS Policy for Information Security.* Refer to the *CMS Information Security Levels* document on cms.hhs.gov/CyberTyger.

1.4 DOCUMENT E-AUTHENTICATION ASSURANCE LEVEL

Section 1.4 applies to any system/application that allows individual web-based access, including Internet, Intranet or Extranet to conduct transactions. 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). Check the appropriate box within the e-Authentication Assurance Level section within the template. If this system does not have web-based transactions, proceed to section 2, Risk Determination Phase. If RACF, Top Secret, Active Directory, or an equivalent authenticating mechanism is implemented for e-authentication of web-users; check the appropriate box.

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 system 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.

1.4.1 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 1 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 1.

Table 1: Potential Impact Categories and Level Definitions

Authentication Error Category	Levels of Potential Impact		
	Low	**Moderate**	**High**
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 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.	At worst, a serious adverse effect on organizational operations or 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.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. (E.g. (i) severe mission 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.

Authentication Error Category	Levels of Potential Impact		
	Low	**Moderate**	**High**
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.

1.4.2 Assign E-Authentication Assurance Level

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 1 to 4 with 1 being minimal and 4 being the highest level of identity assurance.

In assigning the assurance level, the system owner must consider all the direct and indirect consequences as presented in the definitions of the levels. The system 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 five 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:

I. Level 1: Minimal Assurance

At 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 might result in at most, 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.

II. 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 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.

III. 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.

IV. 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 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 2 to determine the level of e-authentication assurance for each transaction type. Using the level of impact, determined in the previous step, assign the assurance level per authentication error category. In some cases (as shown in Table 2), impact may correspond to multiple assurance levels. In such cases, use the system/application context to determine the appropriate assurance level.

Table 2: Assurance Level by Authentication Error Category Impact
(Low, Moderate and High, reflected in light, medium and dark grey, are Impact Levels.)

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

1.4.3 Document Transaction Assurance Level

Complete the columns labeled under "Transaction Assurance Level" in Table 3 with the determined assurance level, corresponding to the category letter, as a result of section 1.4.2, Assign E-Authentication Assurance Level, for each transaction type. Document the highest assurance level for each transaction type in the "Overall" column.

Table 3: Transaction Type Assurance Level Worksheet (not part of the template)

Transaction Type	Transaction Assurance Level						
	A	B	C	D	E	F	Overall

1.4.4 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 3, "Transaction Type Assurance Level Worksheet", from the column labeled "Overall". Complete the column labeled "Assurance Level" in Table 4 with the overall E-Authentication Assurance Level for the system/application.

Table 4: E-Authentication Assurance Level

e-Authentication Assurance Level	

To implement controls that meet with the required standards outlined in National Institute of Standards' (NIST) Special Publication 800-63 "*Recommended Security Controls for Federal Information Systems*", refer to the *CMS Acceptable Risk Safeguards* (ARS) for guidance.

2 RISK DETERMINATION PHASE

The goal of the Risk Determination Phase is to calculate the level of risk for each threat/vulnerability pair based on: (1) the likelihood of a threat exploiting a vulnerability; and (2) the severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of CIA.

This phase will restate the threats identified in the IS Business RA conducted during the investment analysis stage and determine if the level of risk has changed as a result of system level requirements or changes in technologies. If new business risks/vulnerabilities are identified that were unknown when the IS Business RA was conducted, they should also be evaluated in the business risk section and added as a part of this IS RA process. The second half of this phase will shift to identifying and analyzing system risk/vulnerability pairs as described in Section 2.2.

Table 5 will be used to record the threats for both business risks and the systems risks.

Table 5: Risk Determination Table

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level
Business Risk							
System Risk							

The Item Number (Item No.) designated in the left-most column is for reference purposes only. In the business risk section, use the same System Acronym & Sequential Number from the IS Business RA. The system risks for GSS' and MAs that contain multiple sub-systems or applications, the Item Number will consist of sub-system/application prefix and is 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). If the GSS or MA does not have multiple sub-systems or applications, use the system acronym and a sequential number similar to the business risk section. The Item No. is also used in Table 10 in the IS RA Safeguard Determination Phase, to correlate the analysis done in both tables.

2.1 INCORPORATE RISK FROM IS BUSINESS RA

This section restates the threats to the business function from the IS Business RA and incorporates them into the IS RA. In the event that no IS Business RA exists, this methodology will provide the basic steps to perform an assessment. For a complete and concise description, refer to the *CMS Information Security Business Risk Assessment Methodology*. Depending on the stage of SDLC the project is in, some of the business risks may have been mitigated through system requirements. For this reason, the following steps must be completed against each of the threats identified from the IS Business RA.

1. Map the Business Impact and Business Threat to Threat and Vulnerability pair.
2. Identify whether the recommended safeguard(s) to reduce the risk have been implemented.
3. Re-determine the likelihood of threat occurrence given the implementation of the recommended safeguard(s).
4. Re-determine the severity of impact on the business function by threat occurrence.
5. Re-determine the risk level given the implementation of the recommended safeguard(s).

2.1.1 MAPPING BUSINESS RISKS

Map the threats identified in the IS Business RA, that could have the ability to exploit system vulnerabilities. Refer to the *CMS Information Security Threat Identification Resource* for

examples of environmental/physical, human, natural, and technical threats that apply to the Business Impact, where applicable. This step determines if a business threat can be mitigated through system requirements or can be exploited via system vulnerability. If the business threat cannot be adequately mitigated by the system requirements or if the threat can be exploited through a system vulnerability, then the risk must be noted in Table 12, Additional Comments.

2.1.2 INCORPORATE IS BUSINESS RA RISK INFORMATION

For each of the identified risks in the IS Business RA, incorporate business function threat, vulnerability, risk description, and the controls in place into Table 5 under the Business Risk section. For new threats that were not considered during the IS Business RA, or discovered afterwards, list the item number, threat, and vulnerability in the first three columns.

2.1.3 IDENTIFY RECOMMENDED SAFEGUARD(S) IMPLEMENTED

Determine if the recommended safeguards have been implemented. If the recommended safeguard was to insure the system performed some function to mitigate the risk, validate the system requirements were met. If in the implementation phase of the SDLC, validate the test case(s) and the test results. If the recommended safeguard has not been implemented, copy the likelihood, impact severity and threat level from the IS Business RA into the same areas of the table under the Business Risk section. If the risk has been mitigated then proceed to the next step.

2.1.4 DETERMINE THE LIKELIHOOD OF OCCURRENCE ON THE BUSINESS FUNCTION

For each risk that may have a new risk level, determine the likelihood that the threat will exploit the business vulnerability using the information provided in Table 6 below, Likelihood of Occurrence Levels, for guidelines. Complete the column labeled “Residual Likelihood of Occurrence” in Table 10 with the results of this step. Table 6 is also used to determine the “Likelihood of Occurrence” in the “System Risk” section of Table 5 as described in section 2.2.5.

Table 6: 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.
Medium	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

2.1.5 DETERMINE THE SEVERITY OF IMPACT ON THE BUSINESS FUNCTION

For each risk that may have a new risk level, determine the severity of the impact on the business function using Table 7 below, Business Impact Severity Levels. When re-determining the magnitude of severity of the impact on the business function, the existing controls and the business rules as stated in the IS Business RA must be taken into consideration. Complete the column labeled "Impact Severity" in Table 5 with the results of this step.

Table 7: Business Impact Severity Levels

Impact Severity	Description
Insignificant	Will have almost no impact if the threat occurs. Will result in minimal loss of functional integrity. Requires little or no recovery cost.
Minor	Will have some minor effect on the business function. Will not result in negative publicity or political damage, but may cause minor financial loss. Will require only minimal effort to complete corrective actions and continue or resume operations.
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 CMS, and / or notable loss of confidence in the ability for CMS to complete its stated business mission. May result in legal liability, and will require significant expenditure of resources to complete corrective actions and restore operations.
Serious	May cause considerable disruption in the business function 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, and may require recovery in an Alternate Site environment. May result in full compromise of CMS' ability to provide public programs and services, and complete the stated business mission.

2.1.6 DETERMINE THE BUSINESS RISK LEVEL

The risk can be expressed in terms of the likelihood of threat occurrence and severity of business impact. The Level of Risk is the product of the Likelihood of Occurrence and the Impact Severity, as depicted in the equation below:

$$\text{Level of Risk} \equiv \text{Likelihood of Occurrence} \times \text{Impact Severity}$$

For each risk that may have a new risk level, use Table 8, Risk Levels, to determine the level of system risk and record it within the "Business Risk" section of Table 5. Also, this table will be

used to determine the "Risk Level" in the "Business Risk" section of Table 5 as described in section 2.2.7.

The system owner may increase the risk to a higher level depending on the system's security level and the level of compromise if a threat is realized. These actions must be documented in Table 12, Additional Comments.

Table 8: Risk Levels

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

Completion of this step concludes updating the risk level identification for the Business Risks. The following section will guide the system owner through the process of completing the IS RA.

2.2 SYSTEM RISK DETERMINATION

The System Risk Determination Phase is comprised of six steps:

1. Identify potential dangers to information and system (threats).
2. Identify the system weaknesses that could be exploited associated with the threat/vulnerability pair.
3. Identify existing controls to reduce the risk of the threat to exploit the vulnerability.
4. Determine the likelihood of occurrence for a threat exploiting a related vulnerability given the existing controls.
5. Determine the severity of impact on the system by an exploited vulnerability.
6. Determine the risk level for a threat/vulnerability pair given the existing controls.

This six-step process for Risk Determination is conducted for each identified threat/vulnerability pair. These steps are illustrated in the center section of Appendix A: Risk Assessment Process Flow. Use the "System Risk" section of Table 5, to document the analysis performed in this phase.

2.2.1 IDENTIFY SYSTEM ENVIRONMENT THREATS

Identify threats that could have the ability to exploit system vulnerabilities. Refer to the *CMS Threat Identification Resource* for examples of environmental/physical, human, natural, and technical threats that may affect the system. The system owner must consider interconnection

and interdependencies with other systems that may introduce new threats to the system. Therefore, an understanding of the system's interconnections and subordinate processes will provide significant information regarding inherited and additional risks and controls that may affect the system and they must be identified in this section.

Complete columns labeled "Item No." and "Threat Name" in the "System Risk" section of Table 5 with the result of this step.

2.2.2 IDENTIFY SYSTEM VULNERABILITIES

Identify vulnerabilities associated with each threat to produce 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 SDLC may be used to identify vulnerabilities for new systems or systems undergoing major modifications.

Complete the column labeled "Vulnerability Name" in Table 5 with the result of this step.

2.2.3 DESCRIBE RISK

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 column labeled "Risk Description" in the "System Risk" section of Table 5 with the result of this step.

2.2.4 IDENTIFY 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. Existing controls may be management, operational, and/or technical controls depending on the identified threat/vulnerability pair and the risk to the system.

Complete the column labeled "Existing Controls" in the "System Risk" section of Table 5 with the result of this step.

2.2.5 DETERMINE THE 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. The likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access, and existing controls; the presence, motivation, tenacity, strength, and nature of the threat; and the presence of vulnerabilities; and the effectiveness of existing controls.

Refer to the information provided in Table 6, for guidelines to determine the likelihood of occurrence that the threat is realized and exploits the system's vulnerability.

Complete the column labeled "Likelihood of Occurrence" in the "System Risk" section of Table 5 with the result of this step.

2.2.6 DETERMINE THE SEVERITY OF IMPACT

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 Information Security Levels* document and described in the System Documentation Phase of this methodology (Section 1). 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.

Refer to Table 9 for guidelines on system impact severity levels.

Table 9: System Impact Severity Levels

Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

Complete the column labeled “Impact Severity” in the “System Risk” section of Table 5 with the result of this step.

2.2.7 DETERMINE THE RISK LEVEL

The risk can be expressed in terms of the likelihood of the threat exploiting the system vulnerability and the impact severity of that exploitation on the CIA of the system. Also, incorporate the likelihood of threat occurrence and severity of business impact. Refer to the IS Business RA for details. Refer to Table 9 above to determine the level of system risk. The system owner may increase the risk to a higher level depending on the system’s security level and the level of compromise if a threat is realized.

Complete the column labeled “Risk Level” in the “System Risk” section of Table 5 with the result of this step.

3 SAFEGUARD DETERMINATION PHASE

The Safeguard Determination Phase involves identification of additional controls, safeguards or corrective actions to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability pair identified in the Risk Determination Phase 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 for this step is to reduce the risks to low. Use Table 10, to record the identification of new security measures and address the level of risk already assessed for the threat/vulnerability pair. It should also reduce the risk level for both business and systems risks. The residual risk level is determined assuming full implementation of the recommended controls/safeguards.

The Safeguard Determination Phase is comprised of four steps:

1. Identify the controls/safeguards to reduce the risk level of an identified threat/vulnerability pair, if the risk level is moderate or high.
2. Determine the residual likelihood of occurrence of the threat if the recommended safeguard is implemented.
3. Determine the residual impact severity of the exploited vulnerability once the recommended safeguard is implemented.
4. Determine the residual risk level for the system.

These steps are illustrated in the bottom section of Appendix A: Risk Assessment Process Flow. Use Table 10 to summarize the analysis performed during the Safeguard Determination Phase.

Table 10: Safeguard Determination Table

Item No.	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level
Business Safeguards				
System Safeguards				

Use the "Item Number" created for Table 5 to correlate the analysis summarized in both sections of Table 10 for those threat/vulnerability pairs with an associated risk level of moderate or high.

3.1 IDENTIFY RECOMMENDED SAFEGUARDS

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination Phase. 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:

1. Security area where the control/safeguard belongs, such as management, operational, and technical;
2. Method the control/safeguard employs to reduce the opportunity for the threat to exploit the vulnerability;
3. Effectiveness of the proposed control/safeguard to mitigate the risk level; and
4. Policy and architectural parameters required for implementation in the CMS environment.

For Business Risks, it is vital to refer to the IS Business RA for the identified safeguards, and use Table 10 to record these safeguards/controls. Where necessary, add new safeguards that are applicable and feasible.

To determine safeguards for authentication risks resulting from electronic transactions, system owners must consider the entire e-authentication process. The system owner must determine the requirements for each step in the e-authentication/authorization process. This process includes the following steps:

- Initial enrollment,
- Repeat visits,
- Verification of identity,
- Transaction management,
- Long term records management,

- Periodic tests of the system,
- Suspension, revocation, reissue; and
- Audit.

Refer to the *E-Authentication Technical Guidance National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63* for additional details.

Complete the column labeled "Recommended Safeguard" in Table 10 with the result of this step. 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 phase of the assessment and may be further evaluated in risk management activities.

If a complete implementation of the recommended safeguard cannot be achieved in the CMS environment due to management, operational or technical constraints, annotate the circumstances in Table 12, Additional Comments and continue with the analysis.

3.2 DETERMINE RESIDUAL LIKELIHOOD OF OCCURRENCE

Follow the directions described in Section 2.2.5 of the Risk Determination Phase while assuming full implementation of the recommended safeguard.

Complete the column labeled "Residual Likelihood of Occurrence" in Table 10 with the result of this step.

3.3 DETERMINE RESIDUAL SEVERITY OF IMPACT

Follow the directions described in Section 2.2.6 of the Risk Determination Phase while assuming full implementation of the recommended safeguard.

Complete the column labeled "Residual Impact Severity" in Table 10 with the result of this step.

3.4 DETERMINE 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.

Follow the directions described in Section 2.2.7 of the Risk Determination Phase 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.

Complete the column labeled "Residual Risk Level" in Table 10 with the result of this step.

4 RECOMMENDED SAFEGUARD IMPLEMENTATION PHASE

The IS RA process described in this methodology is an integral part of risk management. Risk Management process prioritizes of risks; categorizes of recommended safeguards and the feasibility of their implementation, and document other risk mitigation processes and solutions within the management, operational and technical areas.

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 system 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.

The system 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 system owner should provide a summarized approach for control implementation including all resources. This will be used by CIO/DAA in the Certification and Accreditation process. Note: Currently, there are no assigned DAAs and the CIO performs that role.

The system owner must use the " Item No.", "Threat Name", and "Vulnerability Name", "Risk Description", "Existing Controls" and "Risk level" created for Table 5 as references in Table 11 to correlate the analysis summarized in both tables to the same threat and associated risk level. Complete the column labeled "Implementation Priority" and "Implementation Rationale" in Table 11 with the results of this step.

Table 11: Implementation Analysis Table

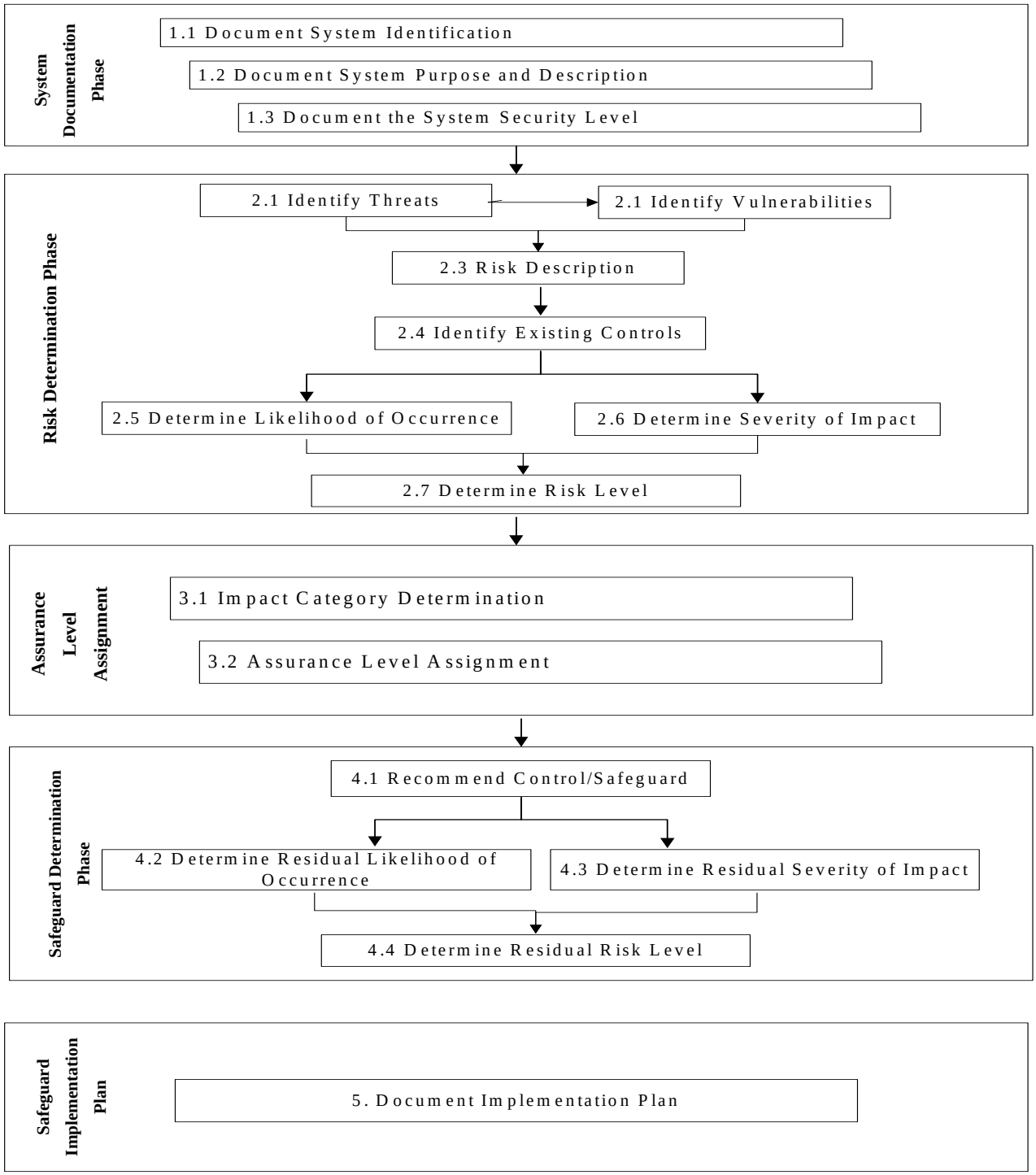
Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Risk Level	Recommended Safeguards	Implementation Priority	Implementation Rationale
IS Business RA Analysis								
IS RA Analysis								

Any additional explanation for the implementation approach and order of priority for the recommended safeguards can be provided in Table 12.

Table 12: Additional Comments

Additional comments for the implementation approach and order of priority for the recommended safeguards (if needed).

APPENDIX A. RISK ASSESSMENT PROCESS FLOW



APPENDIX B. SECURITY IN THE SYSTEM DEVELOPMENT LIFE CYCLE

Although information security must be considered in all phases of the life of a system, the System Development Life Cycle (SDLC) identifies four specific steps that are needed to ensure that information at CMS is properly protected. These include the IS Business RA (Section 10.5 of the Business Case Analysis (BCA)), System Requirements Document, the IS RA and the SSP.

Step 1 - The IS Business RA

Prior to project initiation, the system owner prepares a BCA, which includes the IS Business RA (section 10.5 of the BCA). In this step, the system owner categorizes the data according to sensitivity and identifies high-level security requirements that apply to the system under consideration for development. Information from the Business RA is one of the factors considered in determining if the system will go forward into development and what level of information security will be needed. Elements from the IS Business RA provide the initial input to the IS RA.

Step 2 –System Requirements Document (specifically Security Requirements)

As an initial step of the development process, system requirements are documented for every system. The security requirements serve as a baseline for security within the system. The *CMS Information Security Acceptable Risk Safeguards (ARS*) is the CMS IS minimum security standards and along with the CMS IS policies should be used in defining security requirements. Other requirements may be determined by business or functional requirements.

Step 3 – IS RA

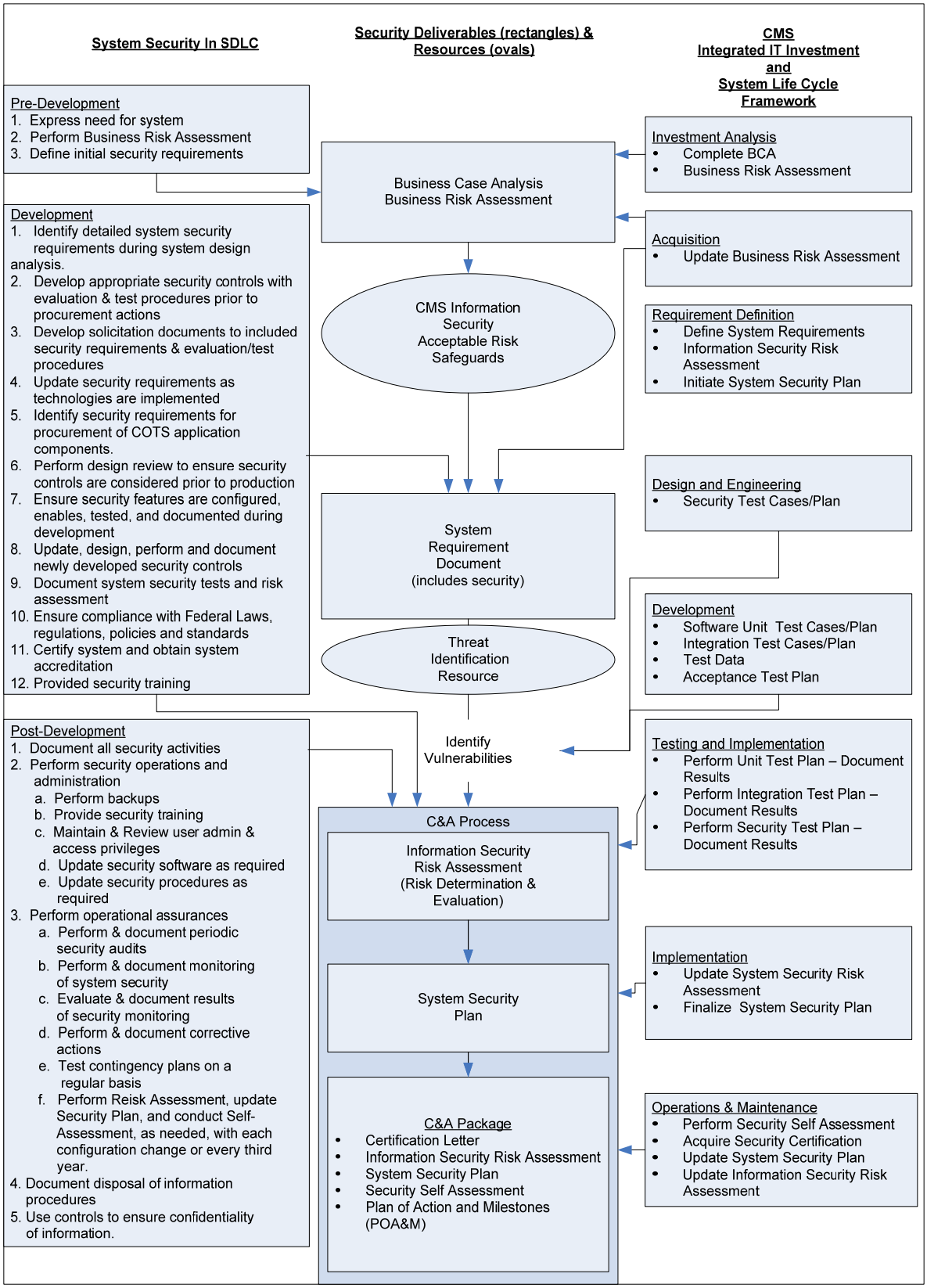
During the development process, a risk assessment is conducted and the resulting IS RA documents the vulnerabilities that have been identified in the system, the risks to the system resulting from the vulnerabilities, and the efforts designed to reduce those risks through the use of safeguards. The IS RA provides input to the IS SSP and CMS IS Certification and Accreditation process.

Step 4 – SSP

The SSP incorporates all of the elements required for the system owner to determine if the system should be certified as meeting both CMS policy and business requirements. Information from the system RA is incorporated into the SSP in Section 2 – Management Controls.

Security steps also correspond to phases in the CMS Integrated IT Investment & System Life Cycle Framework (FRAMEWORK) for system development. The FRAMEWORK is CMS' implementation standard for SDLC and Investment Management and can be found on http://cmsnet.cms.hhs.gov/hpages/oisnew/resources/roadmap/IT_Investment_Mgmt_Process_Guide.pdf. In Figure B-1, the SDLC and FRAMEWORK are shown on the right and left sides, respectively, with the IS deliverables and tools entered in the center section between them. This format illustrates the relationship of the IS tasks to both processes.

Figure B-1. Security in the System Development Life Cycle and CMS' Framework



APPENDIX C. REFERENCES

NIST SP 800-30, Risk Management Guide for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST SP 800-63, Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

OMB M 04-04 E-Authentication Guidance
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

CMS Information Security Incident Handling Procedures
http://cmsnet.cms.hhs.gov/cybertyger/docs/incident%5Fhandling.pdf

CMS IS Terms and Definitions
http://cms.hhs.gov/it/security/docs/termsanddefinitions.pdf

CMS Threat Identification Resource
http://cmsnet.cms.hhs.gov/cybertyger/docs/ref/threat%5Fid%5Fresource.pdf

CMS Information Security Acceptable Risk Safeguards (ARS)
http://cms.hhs.gov/it/security/docs/ars.pdf

CMS Information Security Levels
http://cms.hhs.gov/it/security/docs/ssl.pdf

CMS Integrated IT Investment Management Road Map; August 15, 2001
http://cmsnet.cms.hhs.gov/Framework/misc/IT_Investment_Mgmt_Process_Guide.pdf

CMS System Security Plan Methodology, Version 2.1
http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf

APPENDIX D. INFORMATION SECURITY RISK ASSESSMENT TEMPLATE

The following pages are provided as a template for the IS RA.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

<Office/Center>
<Group Name>
<Address>

<SYSTEM NAME>
Information Security
Risk Assessment (RA)

<Version #.# >
<Month DD, YYYY>
RA Template April 22, 2005, Version 2.1

1 SYSTEM DOCUMENTATION

1.1 SYSTEM IDENTIFICATION

1.1.1 SYSTEM NAME/TITLE

Official System Name	
System Acronym	
System of Records (SOR)	
Financial Management Investment Board (FMIB) Number	
System Type (check one)	☐ GSS ☐ MA ☐ GSS sub-system ☐ MA individual application

1.1.2 RESPONSIBLE ORGANIZATION

Name of Organization	
Address	
City, State, Zip	
Contract Number, Contractor contact information (if applicable)	

1.1.3 INFORMATION CONTACT(S)

Name (System Owner/Manager)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Contractor contact information (if applicable)	

Name (Business Owner/Manager)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Contractor contact information (if applicable)	

Name (System Maintainer Manager)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Contractor contact information (if applicable)	

Name (IS RA Author)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Contractor contact information (if applicable)	

1.1.4 ASSIGNMENT OF SECURITY RESPONSIBILITY

Name (individual[s] responsible for security)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Emergency Contact Information (name, phone and e-mail only)	

Name (Component ISSO)	
Title	
Name of Organization	
Address	
Mail-stop	
City, State, Zip	
Email Address	
Phone number	
Emergency Contact Information (name, phone and e-mail only)	

1.2 SYSTEM PURPOSE AND DESCRIPTION (ASSET IDENTIFICATION)

Identify the assets covered by the IS RA, provide a complete and concise description of the function and purpose of the system and the organizational business processes supported, including functions and processing of data. If it is part of a GSS, include all supported applications, as well as functions and information processed.

[Click here and Type]

1.2.1 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

Provide a complete and concise technical description of the system. Discuss any environmental factors that raise special security concerns and document the physical location of the system. Provide a network diagram or schematic to help identify, define, and clarify the system boundaries for the system, and a general description of the system.

[Click here and Type]

1.2.2 SYSTEM INTERCONNECTION/INFORMATION SHARING

For GSSs or GSS sub-systems, show how the various components and sub-networks are connected and/or interconnected to any other Local Area Network (LAN) or Wide Area Network (WAN). For MAs and MA individual applications provide a description of the system, individual application(s) and/or other software interdependencies.

[Click here and Type]

1.3 SYSTEM SECURITY LEVEL

Describe and document the information handled by the system and the overall system security level as LOW, MODERATE or HIGH. Refer to the *CMS Information Security Levels* document on http://cms.hhs.gov/CyberTyger .

[Click here and Type]

	Information Category	Level
Security Level	[Click here and Type]	[Click here and Type High, Moderate or Low]

1.4 E-AUTHENTICATION ASSURANCE LEVEL

(Check the appropriate boxes.)

☐ *System/Application has web-based access for individuals to conduct transactions;*
☐ *RACF/Top Secret/Active Directory or equivalent is used to authenticate individuals for all web-based transactions;*

OR

☐ *No web-based transactions by individuals. (Proceed to section 2.)*

Determine the required level of e-authentication assurance, based on the impacts of an authentication error, as 1, 2, 3 or 4.

e-Authentication Assurance Level	[Click here and Type 1, 2, 3 or 4]

2 RISK DETERMINATION

The goal of this phase is to calculate the level of risk for each threat/vulnerability pair based on: (1) the likelihood of a threat exploiting a vulnerability; and (2) the severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of confidentiality, loss of integrity and loss of availability. In addition, incorporate the documented threats in the IS Business RA here. Map the Business Impact to Threat and Vulnerability pair
Risk Level = Likelihood of Occurrence X Severity of Impact

Risk Determination Table

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level
Business Risks							
System Risks							

3 RECOMMENDED SAFEGUARDS DETERMINATION

The Safeguard Determination Phase involves identification of additional safeguards to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability pairs identified in the Risk Determination Phase and resulting in moderate and high risk levels.

Safeguard Determination Table

Item No.	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level
Business Safeguards				
System Safeguards				

4 IMPLEMENTATION ANALYSIS

Implementation Analysis Table

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Risk Level	Recommended Safeguards	Implementation Priority	Implementation Rationale
IS Business RA Analysis								
IS RA Analysis								

Additional comments for the implementation approach and order of priority for the recommended safeguards (if needed).