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)
Security and Standards Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Risk Assessment (RA) Methodology

Version # 1.1
September 12, 2002

Table of Contents

Overview

The Centers for Medicare & Medicaid Services (CMS) Information Security Risk Assessment (RA) Methodology presents a systematic approach for the RA process of information computer systems within the CMS environment. This methodology describes the steps to produce an Information Security RA Report for systems that are part of a General Support System (GSS), Major Application (MA) or that are an "Other" System. The Information Security RA Report includes a system overview to provide a basic understanding of the system and its interconnections, and describe the overall system security level. Additionally, the RA Report contains 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 or residual risk level once the recommended safeguards are implemented.

The 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 system's certification and accreditation process as it affects the organization's security posture and management assesses an acceptable level of risk for continuation of operations.

The RA process is presented as the following three phases:

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

The following appendices are included in the methodology to assist the system owner or RA author in the risk assessment analysis and provide further clarification and references to complete the Information Security RA Report:

Appendix A, Risk Assessment Process Flow – Depicts the RA process flow detailed in this methodology for ease of reference.
Appendix B, Security in the System Development Life Cycle – Describes system security deliverables and resources as they relate to the System Development Life Cycle and the CMS Roadmap.
Appendix C, References – Provides links to web sites for documents referred to or used as background in this Information Security RA Methodology.
Appendix D, CMS Information Security RA Template – Facilitates the RA report documentation, and provides a common and consistent format for the Information Security RA report.

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

Purpose

The CMS Information Security RA Methodology has been developed as a tool to guide system owners and RA authors in evaluating and documenting the system's management, operational and technical security environment. This tool describes the steps to produce the CMS Information Security Risk Assessment Report, which is incorporated into the System Security Plan (SSP) and is reviewed during the CMS Information Security Certification and Accreditation process. The system RA process supports risk management in the evaluation of the system(s) risk impact upon CMS' enterprise security model.

CMS requires each system to have an Information Security RA in each of the following instances: new system, operational legacy system, major system modification(s), increase security risks/exposure, increase of overall system security level, serious security violation(s) as described the CMS Computer Security Incident Handling Procedures document, and security evaluations and/or audits. For a new system or a system undergoing a major modification, an RA will be developed as part of the System Development Life Cycle (SDLC) phases. The RA steps are illustrated in Appendix B of this methodology and the RA Template is provided in Appendix D.

Risk Assessment Process

To perform the information security risk assessment, 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, 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.

1 System Documentation Phase

The System Documentation Phase provides background information to describe the system and the data it handles, as CMS assets in support of or in fulfillment of the organization's business mission. This phase establishes a framework for subsequent 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's design and implementation phases of the system. These steps are illustrated in the top section in Appendix A: Risk Assessment Process Flow, Figure A-1.

1.1 Document System Identification

Document the system name, other related information, and the responsible organization. The system must be categorized as part of a General Support System (GSS), Major Application (MA) or be an "Other" Systems, according to the CMS SSP Methodology.

Official System Name	
System Acronym	
System of Records (SOR)	
Financial Management Investment Board (FMIB) Number	
Web Support Team (WST) Number	
System Type (select one)	**GSS, MA or "Other" System**

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

Identify system contacts information for system owner/manager name, business owner/manager, system maintainer manager and RA author. If applicable, provide contractor information, (i.e., contractor name, contract number, contact, e-mail address and phone number, project officer/GTL name, e-mail address and phone number.)

Name of Individual	
Title	
Name of Organization	
Address	
Mailstop	
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	
Mailstop	
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 RA, provide a brief 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.

1.2.1 Document System Environment and Special Considerations

Provide a brief general 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.

1.2.2 Document System Interconnection/Information Sharing

For GSSs, 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 "Other" Systems provide a description of the system and sub-applications or other software interdependencies.

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 confidentiality, integrity and availability, auditability and accountability as dictated by CMS information security policy. Refer to the CMS Information Security Levels document on CMSnet.cms.hhs.gov/CyberTyger.

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 confidentiality, loss of integrity and loss of availability.

The Risk Determination Phase is comprised of six steps:

1. Identify potential dangers to information and system (threats).
2. Identify the system weakness that could be exploited (vulnerabilities) associated to generate 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, Figure A-1. Use the following table, Table 1, to document the analysis performed in this phase.

Table 1. Risk Determination Phase Table

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

The Item Number designated in the left-most column is for reference purposes only. It is assigned in numerical order as rows are added to the table for different threat/vulnerability pairs. The Item No. is also used in Table 5 in the Safeguard Determination Phase, to correlate the analysis done in both tables.

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 environmental/physical, human, natural, and technical threats that may affect General Support Systems, Major Applications, and Other Systems, when applicable. The system owner must consider interconnection and interdependencies with other systems that may introduce new threats to the system under review. Therefore, an understanding of the system's interconnections and subordinate processes, if any, will provide significant information regarding inherited and new 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 Table 1 with the result of this step.

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 1 with the result of this step.

2.3 Describe Risk

Describe how the vulnerability creates a risk in the system in terms of confidentiality, integrity and/or availability elements that may result in a compromise of the system and the data it handles.

Complete the column labeled "Risk Description" in Table 1 with the result of this step.

2.4 Identify Existing Controls

Identify existing controls that reduce: (1) the likelihood or probability of a threat exploiting an 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 Table 1 with the result of this step.

2.5 Determine the Likelihood of Occurrence

Determine the likelihood that a threat will exploit a vulnerability. The likelihood is an estimate of the frequency or the probability of such an event. 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 2 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 Table 1 with the result of this step.

Table 2. 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 one 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

2.6 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 (confidentiality, integrity and availability) 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. 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 3 for guidelines on impact severity levels.

Table 3. 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 Table 1 with the result of this step.

2.7 Determine the Risk Level

The risk can be expressed in terms of the likelihood of the threat exploiting the vulnerability and the impact severity of that exploitation on the confidentiality, integrity and availability of the system. Mathematically, the Risk Level is equal to the Likelihood of Occurrence multiplied by the Severity of Impact in the system's confidentiality, integrity and availability. Table 4 shows risk levels resulting from the affect of both parameters on the risk level. The system owner may increase the risk to a higher level depending on the system's information security level and the level of compromise if a threat is realized.

Table 4. 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

Complete the column labeled "Risk Level" in Table 1 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 pairs identified in the Risk Determination Phase and resulting in moderate or high risk levels. Identification of new security measures should address the level of risk already assessed for the threat/vulnerability pair and should reduce the risk level. 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, Figure A-1.

Table 5 can be used to summarize the analysis performed during the Safeguard Determination Phase.

Table 5. Safeguard Determination Phase Table

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

Use the Item Numbers created for Table 1 as reference in Table 5 to correlate the analysis summarized in both tables to the same threat/vulnerability pair and associated risk level. The Items Numbers here are used to maintain consistency, and ease of reference, and match a recommended safeguard to a threat/vulnerability pair. They refer back to the same item numbers used in the Risk Determination Phase for the threat/vulnerability pairs that resulted in moderate or high risk levels.

3.1 Identify Safeguards

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

Recommended safeguards will address the security category identified during the risk analysis process (confidentiality, integrity and availability) that may be compromised by the exploited vulnerability.

Complete the column labeled “Recommended Safeguard” in Table 5 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 outside of the scope of this methodology.

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 this space and continue with the analysis.

3.2 Determine Residual Likelihood of Occurrence

Follow the directions described in Section 2.4 of the Risk Determination Phase while assuming full implementation of the recommended safeguard.

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

3.3 Determine Residual Severity of Impact

Follow the directions described in Section 2.5 of the Risk Determination Phase while assuming full implementation of the recommended safeguard.

Complete the column labeled "Residual Impact Severity" in Table 5 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 Confidentiality, Integrity and Availability.

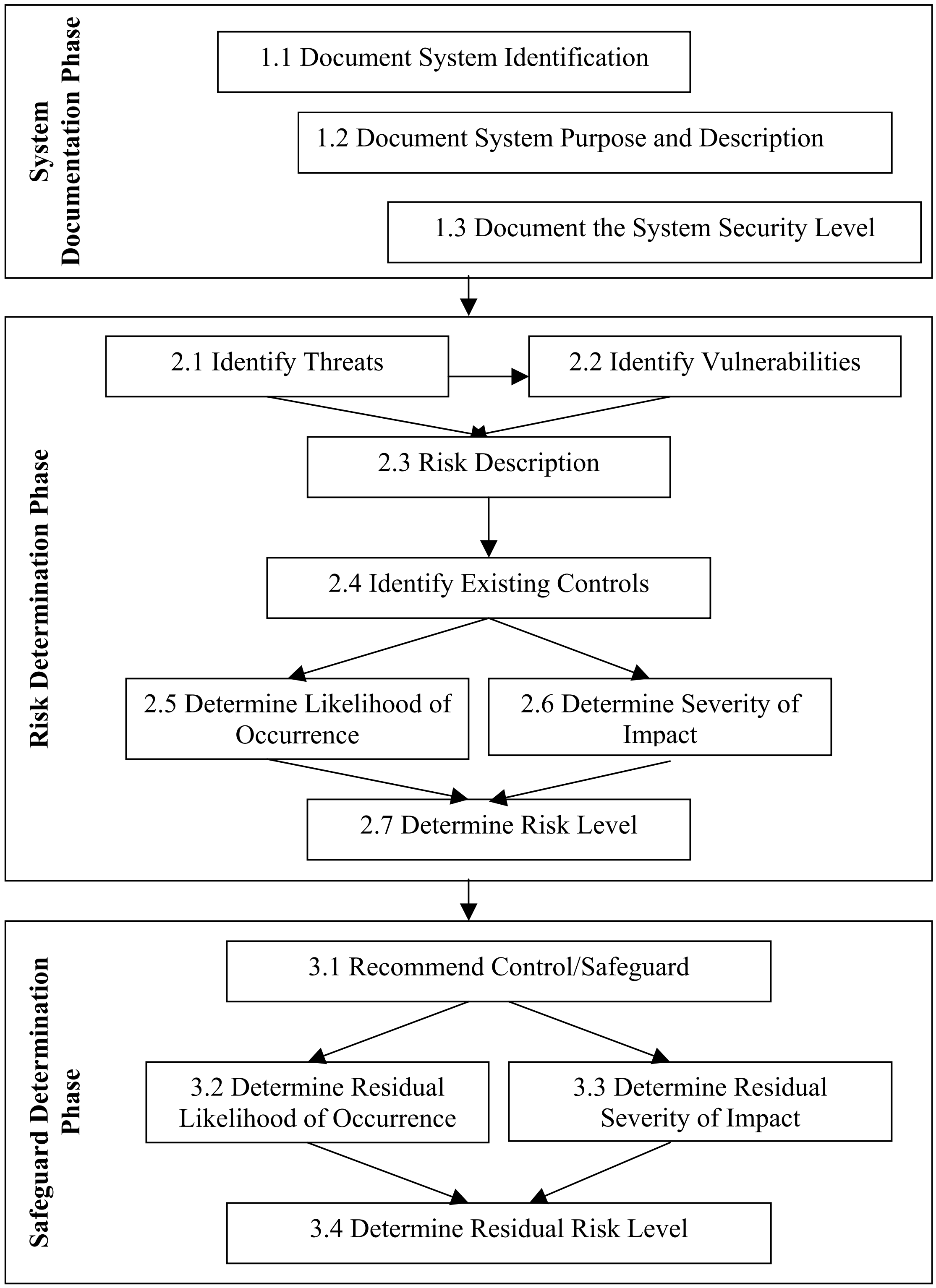
Follow the directions described in Section 2.6 of the Risk Determination Phase to determine the residual risk level once the recommended safeguard is fully implemented.

Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard may reduce the risk level to Low. Annotate with a narrative below the table, if needed, if such special conditions exist.

Complete the column labeled "Residual Risk Level" in Table 5 with the result of this step.

Appendix A: Risk Assessment Process Flow

Figure A-1: 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 identifies four specific steps that are needed to ensure that information at CMS is properly protected. These include the Information Sensitivity Assessment (Section 10.5 of the Business Case Analysis), System Requirements Document, the RA Report and the System Security Plan.

Step 1 - The Information Sensitivity Assessment (ISA)

Prior to project initiation, the system owner prepares a Business Case Analysis (BCA), which includes the ISA (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 ISA 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 ISA provide the initial input to the 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 Minimum Information Security Standards is a tool to assist in defining security requirements. Other requirements may be determined by business or functional requirements.

Step 3 – Risk Assessment Report

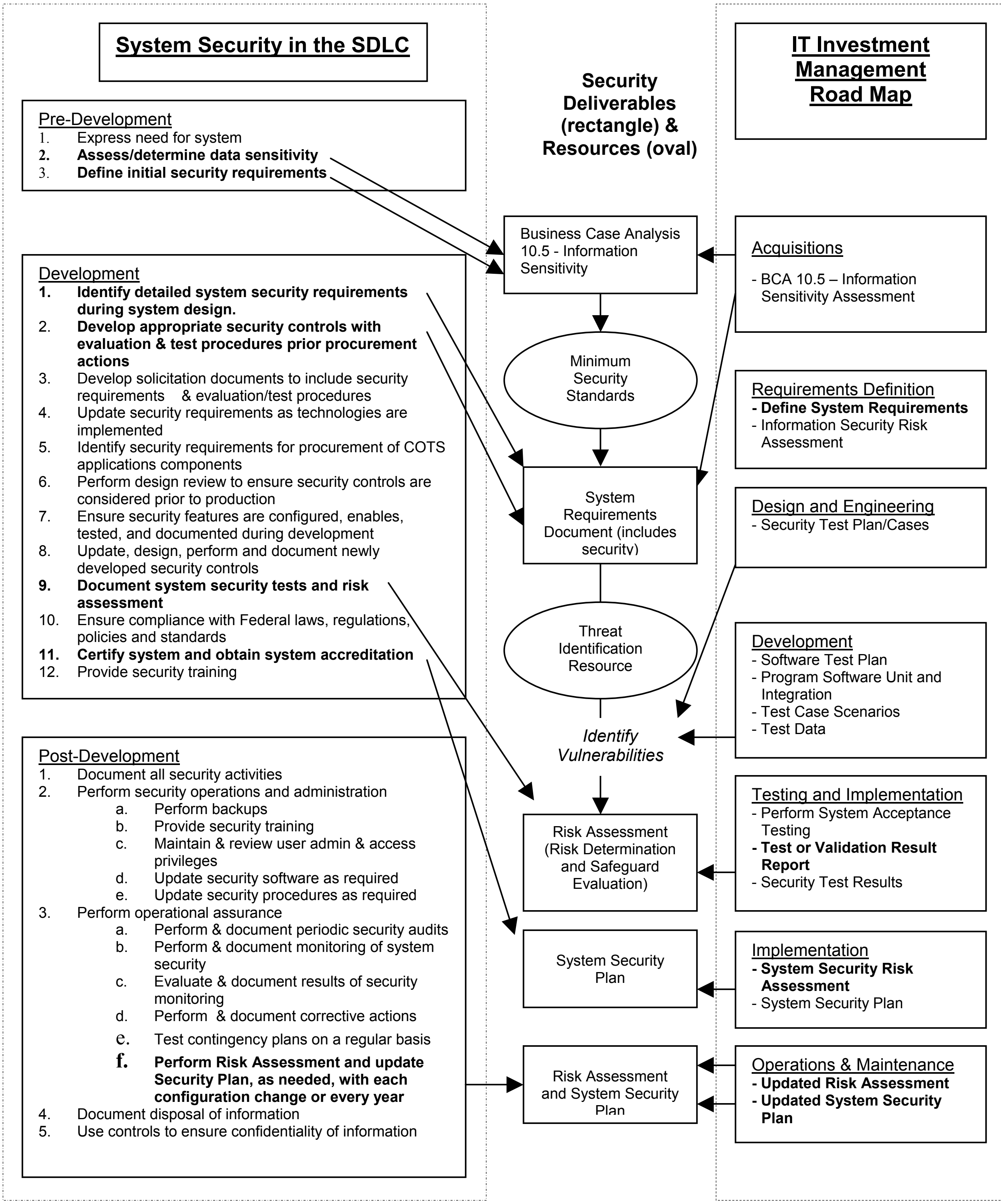
During the development process, a risk assessment is conducted and the result RA Report documents the vulnerabilities that have been identified in the system, the risks to the system resulting from the vulnerabilities and the efforts designed to reduce those risks, through the use of safeguards. The RA Report provides input to the System Security Plan and other risk management activities.

Step 4 – System Security Plan

The System Security Plan 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 RA Report is incorporated into the System Security Plan in Section 2 – Management Controls.

Security steps also correspond to phases in the Integrated IT Investment Management Road Map (ROADMAP) for system development. The ROADMAP is CMS' implementation standard for SDLC and Investment Management and can be found on HCFAnet.HCFA.gov/roadmap/intro/roadmap.htm. In Figure B-1, the system development life cycle and ROADMAP are shown on the right and left sides with the information security deliverables and tools entered in the center section between them. This format illustrates the relationship of the information security tasks to both processes.

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



Appendix C: References

CMS Information Security Levels;
http://cmsnet.cms.hhs.gov/cybertyger/docs/security_levels.pdf

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

CMS System Security Plan Methodology, Version 2.1;
http://hcfanet.hcfa.gov/hpages/ois/ssp/022102_SSP_meth_V2-1.pdf

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

Australian Communications-Electronic Security Instruction 33, Handbook 3: Risk Management; Defense Signals Directorate; http://www.dsd.gov.au/infosec/acsi33/HB3p.pdf

Appendix D: Information Security Risk Assessment Template

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	
Web Support Team (WST) Number	
System Type (select one)	**GSS, MA or "Other" System**

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	
Mailstop	
City, State, Zip	
Email Address	
Phone number	
Contractor contact information (if applicable)	

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

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

Name (IS RA Author)	
Title	
Name of Organization	
Address	
Mailstop	
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	
Mailstop	
City, State, Zip	
Email Address	
Phone number	
Emergency Contact Information (name, phone and e-mail only)	

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

1.2 Asset Identification

Identify the assets covered by the RA, provide a brief 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 brief general 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, 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 “Other” Systems provide a description of the system and sub-applications 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://CMSnet.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]

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. **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

3 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