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)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Business Risk Assessment Methodology

Version 2.1
May 11, 2005

Summary of Changes

V2.1

“Summary of Changes” page added

V2.0

1. No new requirements have been added to this version
2. Content changes are only for clarification.

TABLE OF CONTENTS

OVERVIEW

The Business Risk Assessment (RA) provides decision-makers with the information required to understand the impact of interruptions on business functions and outcomes. This analysis serves as a basis for informed judgments concerning the extent to which action is needed to reduce the level of risk present in a business process.

The Centers for Medicare & Medicaid Services (CMS) *Information Security (IS) Business Risk Assessment (RA) Methodology* presents a systematic approach for the RA process of CMS business functions for Information Security. This methodology describes the steps required to develop an IS Business RA.

The IS Business RA includes an overview section describing the business functions; their supporting processes and resources; and any interdependencies. Further, this section of the report classifies the sensitivity level of the information used by the business process, and the criticality of the business function.

Additionally, the IS Business RA contains a list of threats to the business process; an evaluation of current safeguards, i.e. internal controls; an assessment of the risk level associated with each threat; and the recommended safeguards to reduce the risk exposure to an acceptable level. Business Rules, which govern the business activities, will also be identified and considered when determining potential business impact. A business rule is a statement that defines or constrains some aspect of the business. It is intended to emphasize business structure, or to control or influence the behavior of the business.

The IS Business RA process includes the following four phases:

- Business Function Documentation Phase (to document Business Functions).
- Risk Determination Phase (to document threats to business processes).
- Safeguard Determination Phase (to document internal controls).
- Implementation Analysis Phase (to prioritize risks and determine feasibility of their implementation).

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 and the feasibility of their implementation, and other risk mitigation processes and solutions within the management, operational and technical areas. These risk management activities are performed as part of the IS Certification and Accreditation (C&A) process as it affects the system's security posture within the organization.

The following appendices are included in the methodology to assist the System Owner or IS Business RA author in the risk assessment analysis and provide further clarification and references to complete the IS Business RA:

Appendix A, Risk Assessment Process Flow – Depicts the IS Business RA process flow detailed in this methodology for ease of reference.

Appendix B, Sample Business Threat Identification – A sample to assist System Owners in identifying potential threats to the business function and underlying business processes and resources.
Appendix C, Sample Risk Determination Table
Appendix D, Sample Safeguard Determination Table
Appendix E, Sample Recommended Safeguard Identification – A sample to assist System Owners in identifying additional or different safeguards necessary to reduce the risk level
Appendix F, Sample Implementation Analysis Table
Appendix G, References
Appendix H, IS Business Risk Assessment Template – The template to be used to document IS Business RA.

Refer to the *CMS Information Security Terms and Definitions* document for information security terms used throughout this methodology, http://cms.hhs.gov/cybertyger.

PURPOSE

The *CMS IS Business RA Methodology* has been developed to guide System Owners and IS Business RA authors in conducting and documenting an IS Business RA. A template for the IS Business RA has been provided in Appendix H.

The purpose of an IS Business RA is to:

- Identify and classify the sensitivity of the information to be used in a business function;
- Classify the criticality of a business function;
- Identify the Confidentiality, Integrity and Availability (CIA), and Recoverability requirements associated with the business function;
- Identify threats to the business function;
- Identify the current safeguards in place to mitigate risk; and
- Prioritize risks, analyze the feasibility and effectiveness of recommended safeguards and develop an implementation approach.

The end products of an assessment are the identification and documentation of additional or different safeguards required for protecting and preserving of the security category CIA of the CMS business function and an assessment of the residual risk level once the additional or different safeguards are implemented.

The IS Business RA process is separate and distinct from the IS RA process. The IS RA provides a systematic approach for identifying managerial, operational and technical risks within a CMS system as well as describing mitigation safeguards (particularly internal controls). Whereas the IS Business RA focuses specifically on risks associated with business functions. The IS Business RA assists in identifying the security requirements resulting from security risks, and assists in clarifying the extent to which damage to the business function may occur if a security risk is exploited. The IS Business RA is an integral part of activities performed in the first phase of the System Development Life-Cycle (SDLC). Information gathered prior to and from the IS

Business RA will provide input to the system security plan (SSP), the IS RA, and business continuity planning.

The *CMS IS Business RA Methodology* describes the steps to produce the IS Business RA, which is incorporated into the IS RA and the SSP, and which is reviewed during the IS C&A process. The IS Business RA process supports risk management in the evaluation of the business function's risk impact consistent with the CMS enterprise security model.

CMS requires each System Owner to develop an IS Business RA in response to each of the following events:

- New system, major business process or technology modification(s);
- 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 Procedures*.

For new systems, or technical environments undergoing a major modification, an IS Business RA shall be included in the Business Case Analysis (BCA) during the Investment Analysis Phase of the SDLC. In situations where a BCA is not completed, the IS Business RA must be conducted within the Requirements Analysis Phase of the SDLC.

RISK ASSESSMENT PROCESS

To perform the IS Business RA, the System Owner must identify the potential threats that may cause harm to, or disrupt the business function(s). For each potential threat, the System Owner must also determine the severity of impact upon the business function's CIA requirements, and determine the likelihood the threat being manifested in light of the 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.

Once the risk level is determined for each potential threat, safeguards are identified for threats with Low, Moderate and, High risk levels. Additional safeguards shall be recommended for Moderate and High risk levels. The risk shall be re-evaluated to determine the remaining risk, or residual risk level, after the recommended safeguard is implemented.

1 BUSINESS FUNCTION DOCUMENTATION PHASE

The Business Function Documentation Phase provides background information to describe the proposed system as a CMS asset in support of or in fulfillment of the organization's business mission; each business function supported by the system; and the business resources and information used in supporting each function. This phase establishes the basis for subsequent IS Business RA phases. The Business Function Documentation Phase is designed to identify those areas in which the business functions are most at risk, and describe the safeguards in place or needed to protect those areas.

The System Owner must provide a statement describing *each* business function; the 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. These steps are illustrated in the top section of Appendix A: Risk Assessment Process Flow.

1.1 DOCUMENT SYSTEM IDENTIFICATION

The System Owner shall document the system name and the name of the responsible organization; identify contact information for the System Owner and personnel responsible for security; provide contractor or business partner information, (i.e., contractor name, contract number, contact, e-mail address and telephone number, project officer / Government Task Leader name, e-mail address and telephone number.), if applicable.

1.1.1 IDENTIFY AND DOCUMENT BUSINESS RESOURCES

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 a 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 (check all that apply)	□ GSS □ MA □ GSS sub-system □ 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 name, 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

The System Owner shall provide a statement of purpose and concise description of the CMS system; identify the business functions covered by the IS Business RA; and document the organizational business processes supported by each business function.

1.2.1 IDENTIFY AND DOCUMENT BUSINESS RESOURCES

The System Owner shall provide a general description of the underlying business processes and resources that support each business function, including an explanation of the required inputs, processing functions, personnel and organizational roles and responsibilities, and expected output / product.

The System Owner shall provide a general description of the primary information that will support each business function, and any ancillary information that may be used in any underlying business processes. All other business resources required to support the business function shall be documented, including, but not limited to, user community of the system, users' level of access to the data, facilities, and information technology resources.

The System Owner shall provide a business function model and logical data flow diagram to help identify, define, and clarify the business function boundaries, interdependencies, and data processing logic.

1.2.2 DOCUMENT BUSINESS FUNCTION INTERDEPENDENCIES

Identify and document all CMS business functions/processes that are required and/or support this specific business function (i.e. all other CMS business functions that “feed” this function, or that are “fed” by this function shall be documented).

1.2.3 DOCUMENT OPERATIONAL ENVIRONMENT AND SPECIAL CONSIDERATIONS

Provide a general description of the anticipated technical environment and user community necessary to support the system and business functions. This shall be a high-level analysis, and shall not focus on specific technology, equipment, or software. The technical environment description shall include only broad technological requirements, such as communication requirements, user- interface expectations, and network connectivity requirements. Any factors that raise special security concerns shall be addressed and, if possible, the physical location of the business process and supporting technology shall be documented.

1.3 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 recorded within, such as financial, Medicare, patient, and hospital records.

System 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 and in selecting appropriate security controls and techniques.

Using the *CMS Information Security Levels*, document and the categories of information that support the system in Section 1.2 classify the system security level as Low, Moderate, or High. The *CMS Information Security Levels* document can be downloaded from http://cms.hhs.gov/cybertyger/ .

2 RISK DETERMINATION PHASE

The goal of the Risk Determination Phase is to calculate the level of risk for each potential threat to the business function based on: (1) the likelihood of threat occurrence; and (2) the severity of impact that the threat occurrence would have on the business function in terms of loss of CIA. The Risk Determination Phase comprises seven steps:

Step 1. Identify potential threats to the business function and supporting business processes and resources that could affect the availability and functionality of the application.
Step 2. Analyze the potential impact of each threat to the business function to determine risk.
Step 3. Analyze the potential CMS business impact of each risk.
Step 4. Identify internal controls to reduce the risk of threat occurrence.
Step 5. Determine the likelihood of threat occurrence given the internal controls.
Step 6. Determine the severity of impact on the business function by threat occurrence.

Step 7. Determine the risk level given the internal controls.

This seven-step process for Risk Determination is conducted for each potential threat. These steps are illustrated in the Risk Determination Phase of: Appendix A: Risk Assessment Process Flow. Use Table 1, Risk Determination Table to document the analysis performed in this phase. For an example of this table refer to Appendix C: Sample Risk Determination Table.

Table 1. Risk Determination Table

System Acronym & Sequential Number	Business Function	Threat	Risk Description	Business Impact	Internal Controls	Likelihood of Occurrence	Impact Severity	Risk Level

The System Acronym & Sequential Number designated in the left-hand column is for reference purposes only. It is assigned in numerical order as rows are added to the table for different threats. The “System Acronym & Sequential Number” is also used in the Safeguard Determination Phase; to correlate the analysis documented in both tables, i.e., retain the same System Acronym & Sequential Number when discussing safeguards for Moderate and High risks for ease of traceability.

2.1 BUSINESS FUNCTION

Identify and define the business function that will be reviewed in the context of the next columns (Threat, Risk Description, Business Impact, Internal Controls, Likelihood of Occurrence, Impact Severity and Risk Level). 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 IVR Transcription. Each business function has its own specific processes and associated internal controls. Another example is that of an accounting system with Accounts Payable, Payroll, and General Ledger business functions.

2.2 IDENTIFY THREATS

Identify threats to the business function that may cause disruption in or damage to the business function or supporting business process and resources. Refer to Appendix B: Sample Business Threat Identification of examples of potential threats to the business function. The System 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.

Complete columns labeled “System Acronym & Sequential Number”, “Business Function”, and “Threat” in the Risk Determination Table with the results of this step.

2.3 RISK DESCRIPTION

For each potential threat to the business function identified in the previous step, develop one or more risk descriptions to describe 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.

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.
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.
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.
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.

Complete the column labeled “Risk Description” in the “Risk Determination Table” with the results of this step.

2.4 ANALYZE BUSINESS IMPACT

Business Impact Analysis is developed to determine the impact that could occur due to the compromise of a system. The following parameters should be considered for business impact analysis:

- 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
- Unauthorized release of sensitive information

The negative impact of an event could result in the:

- Inconvenience, distress or damage to standing or reputation,
- Financial loss or agency liability,
- Harm to agency programs or public interests,
- Unauthorized release of sensitive information, or
- Civil or criminal violations.

For each risk description formulated in the previous step, analyze the potential impact of each risk to the CMS business mission.

(Note: these are the continued examples from Section 2.2 above.)

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 may suffer.
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.
	Business Impact:	Employee disciplinary documentation may not be issued on a timely basis resulting in a delayed termination of an undesirable employee.
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.
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.

Complete the column labeled “Business Impact” in Risk Determination Table with the results of this step.

2.5 IDENTIFY INTERNAL CONTROLS

Identify internal controls that reduce the likelihood or probability of a threat occurring, and / or Business Rules that mitigate the impact resulting from threat occurrence.
(Note: these are the continued examples from Section 2.3 above.)

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 may suffer.
	Internal 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.
	Business Impact:	Employee disciplinary documentation may not be issued on a timely basis resulting in a delayed termination of an undesirable employee.
	Internal 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.
	Internal 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.
	Internal Controls:	Business Rule requires two different signatures on a check through separation of duties.

Complete the column labeled "Internal Controls" in Risk Determination Table with the results of this step. The description of the internal controls shall be sufficiently detailed to provide meaningful information to a person unfamiliar with the system. To ensure that this entry in the table is sufficiently descriptive, the author shall refer to a source document, if it exists, or provide a brief summary of the internal controls.

2.6 DETERMINE LIKELIHOOD OF OCCURRENCE

For each threat identified, determine the likelihood that the threat will materialize. 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 the nature of the business function and the type of information and resources supporting the business processes; the presence, motivation, tenacity, strength, and nature of the threat; and, the effectiveness of internal controls and Business Rules. Refer to the information provided in Figure 1, Likelihood of Occurrence Levels for guidelines to determine the likelihood of threat occurrence. Complete the column labeled "Likelihood of Occurrence" in Risk Determination Table with the results of this step.

Figure 1. 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.

2.7 DETERMINE SEVERITY OF IMPACT

Determine the magnitude or severity of impact on the business function if the internal controls and Business Rules are applied and the threat still materializes. Determine the severity of impact for each threat by evaluating the potential loss in each of the areas of confidentiality, integrity, and availability based on the business function criticality and sensitivity levels. The impact can be measured by a partial or full loss of the business function, the inability to complete a CMS business mission, monetary losses, loss of public confidence, or unauthorized disclosure of data. Refer to Figure 2, Impact Severity Levels for guidelines on impact severity levels.

Figure 2. 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. 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.
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.

Complete the column labeled "Impact Severity" in Table 1, Risk Determination Table with the results of this step.

2.8 DETERMINE 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 Severity of Impact in the business function's CIA as follows:

Risk Level = Likelihood of Occurrence X Impact Severity

Figure 3 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 security level and the level of compromise if a threat is realized. However, the System Owner cannot lower the risk level unless the Likelihood of Occurrence and Severity of Impact are also changed.

Figure 3. 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, Risk Determination Table with the result of this step.

3 SAFEGUARD DETERMINATION PHASE

The Safeguard Determination Phase requires the identification of additional controls, safeguards or corrective actions necessary to minimize the likelihood of threat occurrence and resulting business impact for each Moderate or High risk threat identified in the Risk Determination Phase. Identification of new security measures shall address the level of risk previously assessed for the threat and shall reduce the risk level. Assuming all of the recommended controls/ safeguards have been implemented, the residual risk level can be determined.

The Safeguard Determination Phase comprises four steps:

Step 1. Identify the controls / safeguards to reduce the risk level of a threat, if the risk level is moderate or high.
Step 2. Determine the residual likelihood of threat occurrence once the recommended safeguard is implemented.
Step 3. Determine the residual severity of impact on the business function by threat occurrence, once the safeguard is implemented.
Step 4. Determine the residual risk level for the business function.

These steps are illustrated in the Safeguard Determination Phase of Appendix A: Risk Assessment Process Flow.

Table 2 should be completed to summarize the analysis conducted during the Safeguard Determination Phase. For an example of this table refer to Appendix D: Sample Safeguard Determination Table.

Table 2. Safeguard Determination Table

System Acronym & Sequential Number	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level

Use the "System Acronym & Sequential Number" created for Table 1 as references in Table 2 to correlate the analysis summarized in both tables to the same threat and associated risk level. The System Acronym & Sequential Number here are used to maintain consistency, ease of reference, and match a recommended safeguard to a threat. They refer back to the same System Acronym & Sequential Number used in the Risk Determination Phase for threats that resulted in Moderate or High risk levels. Only the Moderate and High risk items will be included in Table 2, Safeguard Determination Table.

3.1 IDENTIFY RECOMMENDED SAFEGUARDS (INTERNAL CONTROLS)

Identify recommended safeguards (internal controls) for each threat with a Moderate or High risk level as identified in the Risk Determination Table. The purpose of the recommended safeguards (internal controls) is to reduce or minimize the level of risk. When identifying a recommended safeguard (internal controls), consider the:

(1) Method the recommended safeguard (internal controls) would employ to reduce the likelihood of threat occurrence;
(2) Effectiveness that would be required of the recommended safeguard (internal controls) to mitigate the risk level; and
(3) Policy and architectural parameters that would be required for implementation in the CMS environment.

Recommended safeguards (internal controls) shall address the threats identified during the risk analysis process. Appendix E: Sample Recommended Safeguard Identification lists selected safeguards (internal controls) but the list identifies **examples only**. Actual recommended safeguards would consider the resources available to maintain the business function, environmental factors, and security inherited from platform systems. Recommended safeguards shall consider industry best practices, and, if applicable, refer to legislative requirements.

Complete the column labeled "Recommended Safeguard Description" in the Safeguard Determination Table with the result of this step. If more than one recommended safeguard (internal control) is identified for the same threat, 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. The description of the recommended safeguard (internal control) shall be sufficiently detailed to provide meaningful information to a person unfamiliar with the system. To ensure that this entry in the table is sufficiently descriptive, the author shall refer to a source document, if it exists, or provide a brief summary of the recommended safeguard (internal control).

Merely selecting appropriate recommended safeguards does not reduce risk. Those safeguards recommended must be implemented effectively through the creation of a Recommended Safeguard Implementation Plan (see section 4). These risk management activities are performed as part of the system's C&A process as it affects the organization's security posture and management determines what the acceptable level of risk for continuation of operations shall be.

3.2 DETERMINE RESIDUAL LIKELIHOOD OF OCCURRENCE

Follow the directions described in Section 2.5 of the Risk Determination Phase, but presume full implementation of the recommended safeguard. Complete the column labeled "Residual Likelihood of Occurrence" in Table 2 with the result of this step.

3.3 DETERMINE RESIDUAL SEVERITY OF IMPACT

Follow the directions described in Section 2.6 of the Risk Determination Phase, but presume full implementation of the recommended safeguard. Complete the column labeled "Residual Impact Severity" in Table 2 with the result of this step.

3.4 DETERMINE RESIDUAL RISK LEVEL

Determine the residual risk level for the threat once the recommended safeguard is implemented. The residual risk level is determined by examining the likelihood of threat occurrence and the business impact severity.

Follow the directions described in Section 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, a recommended safeguard or combination of recommended safeguards may reduce the risk level to Low. Support any annotations with a narrative (entered after the table) if such special conditions exist. Complete the column labeled "Residual Risk Level" in Table 2, Safeguard Determination Table with the results of this step.

4 RECOMMENDED SAFEGUARD IMPLEMENTATION PLAN

The Risk Assessment process described in this methodology is an integral part of risk management. Risk Management also includes prioritization of risks; categorization of recommended safeguards, the feasibility of their implementation, and 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.

The System Owner must use the “System Acronym & Sequential Number”, “Business Function”, and “Risk Description”, “Business Impact”, “Internal Controls” and “Risk level” created for Table 1 as references in Table 3 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 3 with the results of this step. For an example of this table refer to Appendix F: Sample Implementation Analysis Table.

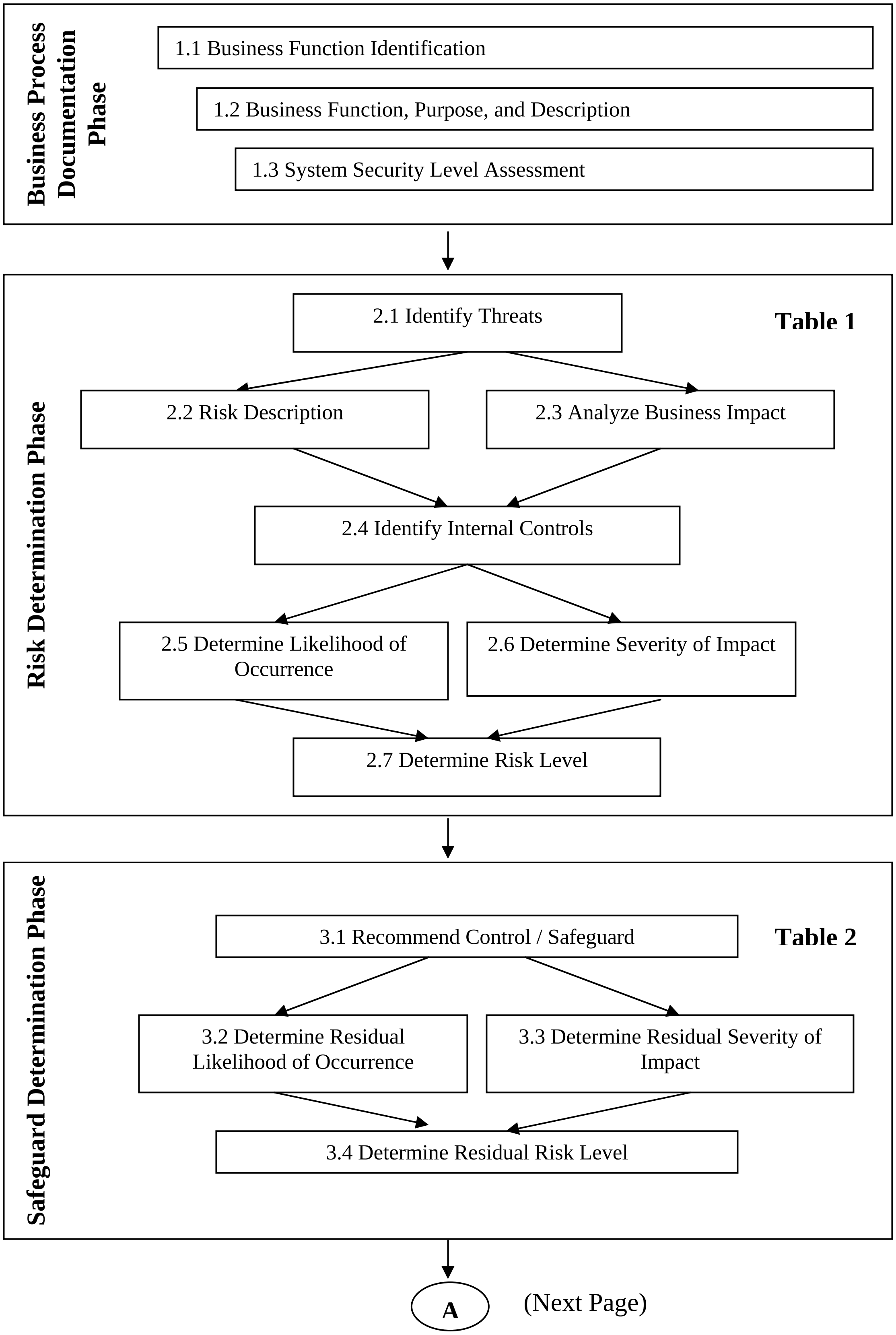
Table 3. Implementation Analysis Table

System Acronym & Sequential Number	Business Function	Risk Description	Business Impact	Internal Controls	Risk Level	Recommended Safeguards	Implementation Priority	Implementation Rationale

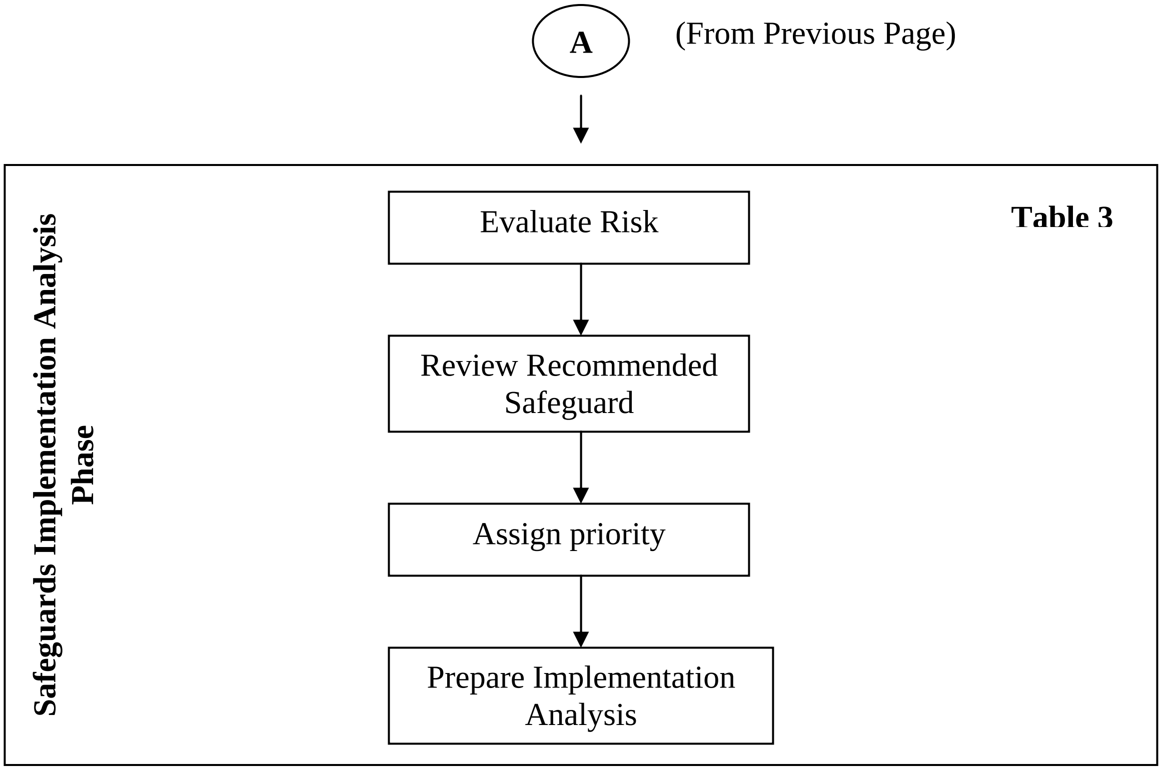
Any additional explanation for the implementation approach and order of priority for the recommended safeguards can be provided in the box below.

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

APPENDIX A: RISK ASSESSMENT PROCESS FLOW


Business Process Documentation Phase
1.1 Business Function Identification
1.2 Business Function, Purpose, and Description
1.3 System Security Level Assessment
Risk Determination Phase
2.1 Identify Threats
Table 1
2.2 Risk Description
2.3 Analyze Business Impact
2.4 Identify Internal Controls
2.5 Determine Likelihood of Occurrence
2.6 Determine Severity of Impact
2.7 Determine Risk Level
Safeguard Determination Phase
3.1 Recommend Control / Safeguard
Table 2
3.2 Determine Residual Likelihood of Occurrence
3.3 Determine Residual Severity of Impact
3.4 Determine Residual Risk Level
A
(Next Page)

Appendix A: Risk Assessment Process Flow (Continued)


A
(From Previous Page)
Safeguards Implementation Analysis Phase
Table 3
Evaluate Risk
Review Recommended Safeguard
Assign priority
Prepare Implementation Analysis

APPENDIX B: SAMPLE BUSINESS THREAT IDENTIFICATION

The following additional business threats are **for example only**:

Threats	Threat Descriptions	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.

APPENDIX C: SAMPLE RISK DETERMINATION TABLE

The following additional business threats are **for example only**:

System Acronym & Sequential Number	Business Function	Threat	Risk Description	Business Impact	Internal Controls	Likelihood of Occurrence	Impact Severity	Risk Level
1	Payroll	Supporting business process not available.	If the employee time-sheet submission function is not available, payroll cannot be completed because there is no basis from which to measure employee compensation.	Employees will not be issued paychecks on time, and employee morale will suffer.	Business Rules are established that enable employees manually to submit time-sheets to management.	Low	Minor	Low

System Acronym & Sequential Number	Business Function	Threat	Risk Description	Business Impact	Internal Controls	Likelihood of Occurrence	Impact Severity	Risk Level
HR 2	Human Resources	HR database is not available.	HR database is not available; no employee information including performance reviews, disciplinary documentation, and achievement memos can be maintained.	Employee disciplinary documentation will not be issued on a timely basis resulting in a delayed termination of an undesirable employee.	Business Rules allow for manual preparation and storage of essential HR documents until the database becomes available.	Low	Damaging	Moderate
MCP 3	Medicare Claims Processing	Information resource erroneous	Given an error in an information resource, an incorrect Medicare payment will be issued.	CMS may incur financial loss.	Business Rules require Medicare claims payment data be reviewed and validated prior to issuing.	Medium	Significant	Moderate

System Acronym & Sequential Number	Business Function	Threat	Risk Description	Business Impact	Internal Controls	Likelihood of Occurrence	Impact Severity	Risk Level
MCP 4	Medicare Claims Processing	Agency-wide failure of data network services.	The loss of that resource results in no Internet, Intranet, e-mail, fax, and other outside connectivity.	Loss of all data network-supported services will impede communications necessary for CMS to conduct business, resulting in failure to process Medicare and Medicaid claims, and the loss of beneficiary confidence.	Business Rules allow hardcopy, communications to internal CMS departments and to external business entities. Internal controls have established emergency communications methods and alternate sites for temporary Internet access.	Low	Serious	High

APPENDIX D: SAMPLE SAFEGUARD DETERMINATION TABLE

The following additional business threats are **for example only**:

System Acronym & Sequential Number	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level
HR 2	Additional Business Rules should be created to ensure undesirable employees who represent potential threats to the organization (either to personnel or agency operations and data) are restricted in their movements and actions pending necessary documentation for employment termination.	Low	Minor	Low
MCP 3	An automated control validates the consistency and accuracy of Medicare claims payment data before payments are issued.	Low	Minor	Low
MCP 4	Each department demonstrating a business need will have Agency-issued cellular telephones available during a major outage.	Low	Significant	Low

APPENDIX E: SAMPLE RECOMMENDED SAFEGUARD IDENTIFICATION

The following additional recommended safeguards are **for example only**:

Recommended Safeguards	Descriptions	Examples
Quality control and validation of information.	Data undergoes a review process to ensure the integrity and validity of information.	Medicare claims payment data is reviewed and validated prior to issuing payment.
Emergency remote access to Mission Critical Major Applications.	If building access is denied, emergency remote access capabilities are in-place to allow for controlled access to Mission Critical Major Applications and Business Rules are established to support the use of these remote access methods.	Alternate geographical locations are established with necessary IT connectivity to CMS.
Manual processes can compensate for the loss of an automated system.	If an automated system upon which the business function relies is unavailable, manual processes exist that ensure the business function can continue to operate.	If the automated time-sheet submission system is unavailable, employees are able manually to submit time-sheets to management.

APPENDIX F: SAMPLE IMPLEMENTATION ANALYSIS TABLE

System Acronym & Sequential Number	Business Function	Risk Description	Business Impact	Internal Controls	Risk Level	Recommended Safeguards	Priority	Implementation Rationale
HR 2	Human Resources	HR database is not available; no employee information including performance reviews, disciplinary documentation, and achievement memos can be maintained.	Employee disciplinary documentation will not be issued on a timely basis resulting in a delayed termination of an undesirable employee.	Business Rules allow for manual preparation and storage of essential HR documents until the database becomes available.	Moderate	Additional Business Rules should be created to ensure undesirable employees who represent potential threats to the organization (either to personnel or agency operations and data) are restricted in their movements and actions pending necessary documentation for employment	1	Easy implementation, very low cost, high likelihood of occurrence results in the implementation priority being high. Furthermore, the implementation of this safeguard shall protect the agency from the actions of the undesirable employees within the agency.

System Acronym & Sequential Number	Business Function	Risk Description	Business Impact	Internal Controls	Risk Level	Recommended Safeguards	Priority	Implementation Rationale
						termination.		
MCP 3	Medicare Claims Processing	Given an error in an information resource, an incorrect Medicare payment will be issued.	CMS may incur financial loss.	Business Rules require Medicare claims payment data be reviewed and validated prior to issuing.	Moderate	An automated control validates the consistency and accuracy of Medicare claims payment data before payments are issued.	1	This risk has been granted a high priority as the occurrence of an error will result in a financial loss to CMS and absence of a control could result in fraudulent activity being performed by claimants.
MCP 4	Medicare Claims Processing	The loss of that resource results in no Internet, Intranet, e-mail, fax, and other outside connectivity.	Loss of all data network-supported services will impede communications necessary for CMS to conduct business, resulting in failure to	Business Rules allow hardcopy, communications to internal CMS departments and to external business entities. Internal controls have established emergency communications	High	Each department demonstrating a business need will have Agency-issued cellular telephones available during a major outage.	2	The presence of internal controls for emergency communications , alternate sites, low likelihood of occurrence and the higher cost of implementation of the

System Acronym & Sequential Number	Business Function	Risk Description	Business Impact	Internal Controls	Risk Level	Recommended Safeguards	Priority	Implementation Rationale
			process Medicare and Medicaid claims, and the loss of beneficiary confidence.	methods and alternate sites for temporary Internet access.				recommended safeguard result in the implementation priority being low even though the risk level is high.

APPENDIX G: REFERENCES

CMS Information Security Levels;
http://cms.hhs.gov/it/security

CMS Integrated IT Investment Management Road Map; August 15, 2001
http://cmsnet.cms.hhs.gov/Framework/misc/IT_Investment_Mgmt_Process_Guide.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/library/infosec/acsi33.html

Financial Management Service Business Risk Assessment Methodology, January 2002 from Department of the Treasury

APPENDIX H: INFORMATION SECURITY BUSINESS RISK ASSESSMENT TEMPLATE

The following pages are provided as a template for the IS Business 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 Business Risk Assessment (RA)

<Version #.# >
<Month DD, YYYY>
RA Template March 17, 2005, Version 2

1 System Documentation

1.1 System Identification

1.1.1 System Name

Official System Name		
System Acronym		
Financial Management Investment Board (FMIB) Number		
System Type (check all that apply)	□ 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	
Mailstop	
City, State, Zip	
E-mail Address	
Telephone Number	
Contractor Contact Information (if applicable)	

Name (IS Business RA Author)	
Title	
Name of Organization	
Address	
Mailstop	
City, State, Zip	
E-mail Address	

Telephone 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	
E-mail Address	
Telephone Number	
Emergency Contact Information (name, telephone and e-mail only)	

Name (Component ISSO)	
Title	
Name of Organization	
Address	
Mailstop	
City, State, Zip	
E-mail Address	
Telephone Number	
Emergency Contact Information (name, telephone and e-mail only)	

1.2 System Purpose and Description

[Click here and Type]

1.2.1 Business Resources

[Click here and Type]

1.2.2 Business Function Interdependencies

[Click here and Type]

1.2.3 Operational Environment and Special Considerations

[Click here and Type]

1.3 System Security Level Assessment

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

2 Risk Determination

System Acronym & Sequential Number	Business Function	Threat	Risk Description	Business Impact	Internal Controls	Likelihood of Occurrence	Impact Severity	Risk Level

3 Safeguard Determination

System Acronym & Sequential Number	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level

4 Implementation Analysis

System Acronym & Sequential Number	Business Function	Risk Description	Business Impact	Internal Controls	Risk Level	Recommended Safeguards	Implementation Priority	Implementation Rationale

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