



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

CMS REPORTING PROCEDURE FOR INFORMATION SECURITY (IS) ASSESSMENTS

March 19, 2009

Version 5.0 Final

SUMMARY OF CHANGES

1. The *CMS Reporting Procedure for IS Assessments*, v5, dated March 19, 2009 replace the *CMS Reporting Standard for Information Security Testing*, v4, dated July 15, 2005.
2. Significant modifications have been made to the *CMS Reporting Procedure for Information Security (IS) Assessments*. Therefore, all sections of this document have been reviewed and updated.”

EXECUTIVE SUMMARY

The *Centers for Medicare & Medicaid Services (CMS) Reporting Procedure IS Assessments*, hereinafter known as “*The Reporting Procedure*”, is the CMS-established standard and guide which all IS Assessment Reports shall follow. *The Reporting Procedure* ensures that each of the three (3) phases of an IS assessment is addressed adequately within the IS Assessment Report and ensures consistency of reports throughout CMS. *The Reporting Procedure* provides a specific format, with instructions, for writing an IS Assessment Report. *The Reporting Procedure* applies to everyone who has responsibility for writing an IS Assessment Report.

The Reporting Procedure is divided into five (5) sections. Section 1-*Introduction*, presents the purpose, the core requirements and considerations, the goals and objectives, and the roles and responsibilities of individuals in reporting IS assessment results. Section 2-*Reporting Process*, defines the template use and reporting perspective. Section 3-*Report Structure*, addresses the executive summary, introduction, detailed findings, and appendices and attachments within the *CMS IS Findings Report Template for Applications*, or *CMS IS Findings Report Template for Business Partner Sites / Infrastructure*. Section 4-*Documenting Risks*, addresses findings number, risk statement, security control family, references, determination guidelines, risk description, suggested corrective action, and status. Section 5-*Security Assessment Report Package*, outlines the two versions of the IS Assessment Report packages and provides details regarding the proper format and content of these packages.

TABLE OF CONTENTS

CMS REPORTING PROCEDURE FOR INFORMATION SECURITY (IS) ASSESSMENTS.....	1
EXECUTIVE SUMMARY	II
1. INTRODUCTION	1
1.1. PURPOSE	1
1.2. CORE REQUIREMENTS AND CONSIDERATIONS	1
1.3. GOALS & OBJECTIVES	2
1.4. ROLES & RESPONSIBILITIES	3
2. REPORTING PROCESS.....	5
2.1. TEMPLATE USE	6
2.2. REPORTING PERSPECTIVE.....	6
2.2.1. KEY COMPONENTS.....	6
2.2.2. RISK ASSOCIATION.....	7
3. REPORT STRUCTURE	8
3.1. EXECUTIVE SUMMARY	9
3.2. INTRODUCTION	9
3.3. DETAILED FINDINGS.....	9
3.3.1. PROCEDURE FOR SECURITY ASSESSMENT.....	10
3.3.2. PROCEDURE FOR IS ASSESSMENT REPORTING.....	10
3.3.3. BUSINESS RISKS	10
3.3.4. RE-ASSIGNED BUSINESS RISK	10
3.4. APPENDICES AND ATTACHMENTS.....	11
3.4.1. CAP MANAGEMENT WORKSHEET.....	11
3.4.2. CAP REVIEW WORKSHEET.....	11
4. DOCUMENTING BUSINESS RISKS.....	12
4.1. FINDING NUMBER	12
4.2. BUSINESS RISK STATEMENT	13
4.3. SECURITY CONTROL FAMILY	13
4.4. REFERENCES.....	14
4.5. DETERMINATION GUIDELINES	14
4.5.1. RISK LEVEL ASSESSMENT.....	14
4.5.2. EASE-OF-FIX ASSESSMENT	19
4.5.3. ESTIMATED WORK EFFORT ASSESSMENT.....	21
4.6. BUSINESS RISK DESCRIPTION	21
4.6.1. TECHNICAL FINDING.....	21
4.6.2. PROCEDURAL FINDING	22
4.7. SUGGESTED CORRECTIVE ACTIONS.....	22
4.8. STATUS	23
5. SECURITY ASSESSMENT REPORT PACKAGE.....	24
5.1. FINAL REPORT PACKAGE	24
5.2. FINAL BOOK PACKAGE	25
5.2.1. COMMUNICATIONS.....	25
5.2.2. WORKING PAPERS.....	26
5.2.3. DOCUMENTATION.....	27
5.3. DELIVERABLE FORMATTING	28
APPENDIX A: CMS IS FINDINGS REPORT TEMPLATE.....	29

APPENDIX B: CMS FINDINGS NUMBERING STANDARD31
APPENDIX C: CAP MANAGEMENT34
APPENDIX D: RESOURCES & REFERENCES39
APPENDIX E: ACRONYMS40

TABLES

Table 1: Roles & Responsibilities for Reporting.....3
Table 4: Impact Severity Classifications17
Table 5: Risk Level Classifications.....18
Table 6: Risk Level Definitions18
Table 7: Ease-of-Fix Assessment19
Table 8: Estimated Work Effort Rating21

FIGURES

Figure 1: IS Assessment Reporting Process5

1. INTRODUCTION

The *CMS Reporting Procedure for Information Security (IS) Assessments* establishes the standard report template, and provides guidance for CMS employees and CMS contractors in documenting and reporting security assessment results. The *CMS Reporting Procedure for IS Assessments*, hereinafter known as "The Reporting Procedure", is the model for documenting and reporting CMS IS assessment. To provide a complete IS assessment program CMS has developed the documents listed hereafter that each of which includes information sufficient to support risk analysis; to track vulnerabilities; and to facilitate the development of a Corrective Action Plan (CAP) for each risk identified during the assessment:

- *CMS IS Assessment Procedure*
- *CMS IS Assessment Plan Template*
- *CMS Application Assessment Findings Report Template*
- *Infrastructure Data Center Assessment Findings Report Template*

The types of information to be included within an IS Assessment Report are consistent with, the National Institute of Standards and Technology (NIST), Federal Information System Controls Audit Manual (FISCAM), and CMS IS policy and standards requirements.

1.1. PURPOSE

The reporting model is the standard for documenting and reporting CMS IS assessment results, such that:

- (1) Security assessment results of technically and administratively unrelated information systems are presented in a consistent format, independent of hardware and software configurations, management processes, or organizational hierarchy;
- (2) The effectiveness of security controls implemented on technically and administratively unrelated information systems can be evaluated comparatively, with respect to information sensitivity level; and
- (3) The ability to gauge the effectiveness of security controls, security management processes, and security improvements is enhanced.

1.2. CORE REQUIREMENTS AND CONSIDERATIONS

In support of the CMS mission, sensitive and critical information is processed, stored and transmitted through a complex infrastructure of information systems. To support existing business requirements, CMS requires the use of diverse information technology components and platforms. To ensure that the confidentiality, integrity and availability of the information system are protected adequately, CMS must implement effective management, operational and technical security controls that reduce risk to an acceptable level. Information security assessments are

required to evaluate the implementation of security controls, to validate their effectiveness, and to identify any residual vulnerability in the information system in spite of those controls.

CMS expects security assessment results to be prepared in a manner that conveys sufficient information to CMS management and to their associated business partners, who shall then use the results to improve internal risk management processes and render informed, risk-based decisions. To achieve consistent reporting across diverse business functions, information technology platforms, and business units, the reporting model must be independent of the CMS business and technological infrastructures. CMS understands that it is critical for the reporting of CMS risks to be based on the analysis of the potential business impact and threat exposure if a technical or procedural security vulnerability is exploited. The business impact depends substantially upon the sensitivity designation of the information at risk of disclosure or modification.

The Reporting Procedure establishes clear guidelines to ensure that security controls for information with corresponding sensitivity levels are measured consistently, and that security testing of all information systems are reported in a comparative fashion. *The Reporting Procedure* further establishes standards for assessing the potential business impact and threat exposure for all vulnerabilities identified during an assessment.

1.3. GOALS & OBJECTIVES

The Reporting Procedure establishes a reporting model that meets the following objectives:

- 1) Is flexible enough to apply to all security assessments of current and future CMS infrastructures supporting CMS information systems;
- 2) Is specific enough to provide accurate results and comparative measurements for all types of security assessments, regardless of systems reviewed;
- 3) Is specific enough to enable CMS to compare security assessment results over time, and to identify categorical improvements or deteriorations;
- 4) Is easy to implement, use, and understand and does not require undue training and preparation time and is readily adaptable to the CMS environment, including CMS business partners and does not substantially increase the work effort of CMS staff or independent security testers;
- 5) Is precise enough to clearly define the processes and responsibilities for security assessment reporting, with firm guidelines for assessing risk level and remediation effort;
- 6) Is consistent, such that similar assessment results are reported in a uniform manner, regardless of tester or information system; and
- 7) Is internally consistent, such that terminology is defined and utilized in a consistent manner.

1.4. ROLES & RESPONSIBILITIES

The IS assessment process outlined in the *CMS Information Security (IS) Assessment Procedure* is reliant upon: (i) the capability, competence and consistency of the Evaluator(s) performing assessment activities; (ii) the cooperation of the Business Owner(s) of the system being evaluated; and (iii) the facilitation of testing activities by appropriate CMS personnel. The Roles and Responsibilities that support reporting are provided in Table 1: Roles and Responsibilities for Reporting.

Table 1: Roles & Responsibilities for Reporting

ROLE	RESPONSIBILITIES
CMS IS Management (Chief Information Officer (CIO), Chief Information Security Officer (CISO))	<ul style="list-style-type: none"> • Implements the CMS IS Certification & Accreditation (C&A) Program and manage the C&A Program tasks • Develops and maintain IS policies, procedures, and control techniques to address system security planning • Utilizes an independent assessment in determining accreditation decisions
Information System Security Officer (ISSO) / System Security Officer (SSO)	<ul style="list-style-type: none"> • Collaborates with the Business Owner and the System Developer / Maintainer to ensure internal system controls are implemented properly and conform to CMS IS policies and standards, and fulfill C&A requirements • Partners with the Facilitator for the successful completion of the IS assessment. • Manages the identification, implementation, and assessment of common security controls
Business Owner	<ul style="list-style-type: none"> • Ensures that the system is deployed, and operated according to the agreed-upon security requirements • Ensures the Assessment documents are developed to include the following: <ul style="list-style-type: none"> • <i>CMS IS Assessment Procedure;</i> • <i>CMS IS Assessment Plan Template;</i> • <i>CMS Application Assessment Findings Report Template;</i> and • <i>Infrastructure Data Center Assessment Findings Report Template.</i> • Selects the Evaluator and oversee the Evaluator’s performance • Assists in the identification, implementation, and assessment of common security controls.
Facilitator	<ul style="list-style-type: none"> • Initiates the IS assessment project • Coordinates the planning and execution of the IS assessment • Approves final deliverables
Evaluator	<ul style="list-style-type: none"> • Conducts the necessary IS assessments of the system to verify controls have been implemented properly • Conducts interviews of key personnel who have a working knowledge

ROLE	RESPONSIBILITIES
	of controls implemented and documentation being reviewed <ul style="list-style-type: none">• Reviews all documentation pertaining to the system under review• Refrains from conducting any assessment activities for which they are not competent to carry out (e.g. a mainframe expert should not conduct mid-tier testing), or from conducting the same in a manner which may compromise the information system being assessed• Prepares an IS Assessment Report that communicates how CMS critical systems and/or data confidentiality, integrity and/or availability will be impacted if a known threat exploits an identified vulnerability

The roles and responsibilities of the Evaluator, Facilitator and the Business Owner of the evaluated information system will be distinct and will not overlap or conflict with any other role or responsibility.

2. REPORTING PROCESS

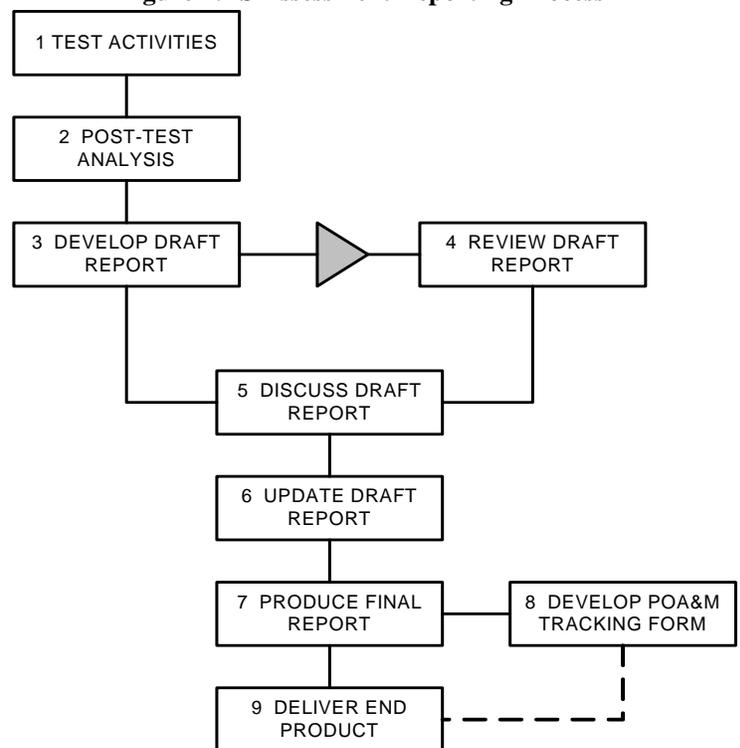
The Business Owner selects the Evaluator and oversees the performance of the Evaluator as detailed in the *CMS IS C&A Program Procedure*¹.

The Evaluator shall conduct security assessments to validate the effectiveness of management, operational, and technical security controls implemented to protect a CMS information system. Technical or procedural vulnerabilities discovered through security testing, reported as Business Risk findings, reveal those areas where the Evaluator has determined that the implemented controls are inadequate. Each finding shall be described in a manner that will explain how the CMS business mission may be impacted if a known threat exploits an identified vulnerability. The Evaluator shall suggest reasonable and appropriate corrective actions that will mitigate the impact of the vulnerability to a Low Risk and that will potentially close the finding.

The Evaluator shall use *The Reporting Procedure* to document the results of a completed assessment. The following procedures, as represented in Figure 1, provide guidance for the creation of an IS Assessment Report:

1. **TEST ACTIVITIES:** The Evaluator shall conduct an IS assessment and gather data.
2. **POST-TEST ANALYSIS:** The Evaluator shall review and analyze the data gathered.
3. **DEVELOP DRAFT REPORT:** The Evaluator shall develop a draft IS Assessment Report, marked as such, and deliver the draft version to CMS.
4. **REVIEW DRAFT REPORT:** The Facilitator shall review the draft IS Assessment Report, provide feedback to the report's author, and, if necessary, schedule a meeting to discuss open issues or to clarify findings.
5. **DISCUSS DRAFT REPORT:** The Facilitator, Business Owner and Evaluator, and all other Security Test &

Figure 1: IS Assessment Reporting Process



¹ If an independent Evaluator is required for a System Test & Evaluation (ST&E) or an annual FISMA assessment, the Business Owner should coordinate through Director Enterprise Architecture and Strategy Group (EASG), Office of Information Services (OIS) and the CMS Chief Information Security Officer (CISO). If the independent testing is not performed through the standard OIS contract vehicles, the Business Owner must contact OIS, Director EASG and the CMS CISO in order to ensure the C&A requirements for independence and testing will be met.

Evaluation (ST&E) stakeholders shall meet to discuss the draft IS Assessment Report and to resolve any issues with the draft report. If necessary, the Business Owner may submit additional documentation.

6. UPDATE DRAFT REPORT: The Evaluator shall make any required revisions to the report.
7. PRODUCE FINAL REPORT: The Evaluator shall produce a final IS Assessment Report, labeled accordingly.
8. DEVELOP POA&M TRACKING FORM: The Evaluator shall prepare and submit a Plan of Action & Milestone (POA&M) tracking form along with the final IS Assessment Report (see *CMS POA&M Guidelines*).
9. DELIVER END PRODUCT: The Evaluator shall deliver the Final IS Assessment Report to the Facilitator, followed by a Final Security Assessment Package which shall include the report and all working papers in hard copy and electronic format as applicable including, but not limited to, all test results, notes, and screenshots.

2.1. TEMPLATE USE

The Evaluator shall use the standard *CMS IS Findings Report Template for Applications* and the *CMS IS Findings Report Template for Business Partner Sites / Infrastructure* to report deficiencies in the environment. The templates include a section that addresses each finding discovered during the testing process, and details the business risk to CMS. The standard report format will enable CMS to review the results of security assessments performed on unrelated technical systems in a uniform manner. The standard format ensures that all assessment results are subject to identical assessment guidelines, and that reports include the same types of information.

2.2. REPORTING PERSPECTIVE

The Facilitator shall afford the Evaluator sufficient latitude and flexibility in addressing the test results from a business or technical perspective. The Evaluator shall document the result in a clear and concise way that will convey the results of the testing. The content of the report will reflect all weaknesses identified during the testing. The discretion granted must be limited to reporting the content of the results in an unbiased, objective manner without preferential language. The Determination Guidelines in Section 4.5 permit an acceptable level of discretion and provide adequate flexibility.

2.2.1. KEY COMPONENTS

The key components of an IS Assessment Report are:

- The description of risks;
- The assignment of finding numbers;
- The assignment of a risk level;
- The evaluation of the complexity of mitigation efforts; and
- An estimation of the work effort required to implement reasonable and appropriate controls to address the vulnerability

2.2.2. RISK ASSOCIATION

The Evaluator shall associate each Business Risk with at least one (1) control from one (1) of the control families identified in the *CMS Policy for the Information Security (IS) Program (PISP)*, the appropriate e-Authentication elements from *CMS Information Security (IS) Acceptable Risk Safeguards (ARS) including the CMS Minimum Security Requirements (CMSR)* and the *Business Partner System Security Manual (BPSSM)*. Associating each risk with a control will assist CMS in evaluating, monitoring, and comparing the effectiveness of security controls across diverse operating environments and platforms. By categorizing the risks into security control families, CMS management will be able to identify categorical weaknesses common to related and unrelated information systems, and to dedicate resources to those control families that, if strengthened, will mitigate the greatest number of vulnerabilities.

3. REPORT STRUCTURE

The structure of the IS Assessment Report will allow the Evaluator to communicate the assessment results to several audience levels, ranging from technical staff to CMS Executives. The IS Assessment Report shall be prepared in a manner that:

- 1) Provides factual findings in accordance with the Rules of Engagement (RoE)²;
- 2) Enables management to render informed decisions regarding the application of resources and staffing to correct system weaknesses and vulnerabilities; and
- 3) Supports the on-going security review processes and the Operations and Maintenance (continuous monitoring) phase of the *CMS Integrated IT Investment & System Life-Cycle Framework*. (The Frame work)

The IS Assessment Report shall enable high-level audiences to understand, quickly and proficiently, the potential impact of the results on the CMS mission and the supporting business processes. Likewise, the report shall present information that enables technical personnel to understand the details of a given vulnerability in order to plan appropriate corrective action.

To accommodate the competing needs of potential audiences, the report format shall provide an initial discussion of the “big picture,” followed by technical details at a lower level. Even if there are no findings to report, the IS Assessment Report must indicate the events of the test and reflect what tests the Evaluator conducted that resulted in a lack of security-related issues.

The decision to include graphs within the IS Assessment Report depends primarily upon a determination of whether the visual tools are likely to add value to the report. If the graphs will provide CMS management with meaningful information that will help conceptualize and appreciate the significance of the test results, the Evaluator may include graphs in the report. A maximum of two (2) visual graphs may be included within the IS Assessment Report, where appropriate. Additional graphics must be relevant to the assessment and shall be included as an appendix to the IS Assessment Report. A sample of appropriate are the following:

- Distribution of Business Risks between High Risk, Moderate Risk, and Low Risk; and
- Breakdown of the weaknesses identified per security control family.

The following sections identify and describe briefly the components of the *CMS Application Assessment Findings Report Template* and the *CMS Infrastructure Data Center Assessment Findings Report Template*.

² Refer to *CMS IS Assessment Procedure* for more information.

3.1. EXECUTIVE SUMMARY

The Executive Summary shall provide a high-level narrative description of the major Business Risks identified during the assessment. The primary audience for the Executive Summary is CMS IS management. The Executive Summary shall, at a minimum:

1. Provide a brief statement of the background for the IS assessment;
2. Provide a brief statement of the scope of the IS assessment;
3. Briefly summarize the significant vulnerabilities, and their potential impact to the system's business function and CMS mission, identified during the test;
4. Recommend, at a high-level, strategic options or corrective actions necessary to close or reduce the impact of each type of vulnerability;
5. Identify any significant assessment related issues that helped or hindered the security testing;
6. Relate the status of findings and associated CAPs from previous tests; and
7. Describe any observed vulnerability trends or categorical weaknesses.

The Evaluator shall minimize the technical details contained within the Executive Summary, but shall provide sufficient detail to support the brief summary of the significant vulnerabilities and their potential impact on the information system. The Evaluator shall reserve in-depth technical details for inclusion in the Business Risk descriptions contained within each finding.

3.2. INTRODUCTION

The "Introduction" to the IS Assessment Report shall include:

1. A brief description of the security assessment engagement, including the information system that was tested, the specific security controls and control families that were tested, the purpose of the assessment and the scope of the assessment;
2. A description of the business function supported by the system or application that was assessed;
3. The name of the organization which conducted the assessment; and
4. The period of performance of the assessment, including the specific dates of any on-site assessment.

3.3. DETAILED FINDINGS

The "Detailed Findings" section shall include:

1. A description of how the assessment was conducted, including what tools and procedures were used by the Evaluator;
2. A description of how the business risks have been analyzed and documented; and
3. All individual business risks identified during the security assessment.

3.3.1. PROCEDURE FOR SECURITY ASSESSMENT

The IS Assessment Report shall identify the tools and test procedures used to assess the information system. The IS Assessment Report shall state that the assessment was conducted in accordance with the *CMS IS Assessment Procedure*.

This sub-section shall include methods of discovery and any tools used during discovery. The Evaluator shall present the list of tools, and the purpose of each tool, within a table format.

3.3.2. PROCEDURE FOR IS ASSESSMENT REPORTING

The Evaluator shall describe the criteria for measuring the Risk Level, Ease-of-Fix, and Estimated Work Effort metrics that are included within each Business Risk. The language provided in the templates shall be the standard language (i.e. “boilerplate”) for all IS Assessment Reports.

3.3.3. BUSINESS RISKS

The individual Business Risks provide technical details and analyses of each vulnerability discovered during the security assessment, and contain suggestions for corrective actions that will close or reduce the impact of each vulnerability.

The Business Risk template is divided into the following sections:

1. Control Family;
2. Control Reference;
3. Risk Level, Ease-of-Fix, Level-of-Effort;
4. Technical details of each identified vulnerability; and
5. Step-by-step suggestions for corrective actions.

Refer to Section 4 for information on how to document each Business Risk.

3.3.4. RE-ASSIGNED BUSINESS RISK

During the draft report review meeting, the Evaluator, the Facilitator, Business Owner and all other assessment stakeholders may determine that the Business Owner is not fully responsible for the risk associated with a particular finding, e.g., a flaw in the Medicare Data Communications Network (MDCN) was discovered in the transmission of data between Data Centers. Such an evaluation should be predicated on who is responsible for the CAP that will be generated for the finding, and on who is responsible for the Business Risk. However, this may require more internal discussion within CMS as to the responsible Business Owner before a final disposition is given to the Evaluator.

Findings that are re-assigned to another organization are to be included in the Final IS Assessment Report, but shall be in a separate section that identifies the organization that is responsible for such findings.

3.4. APPENDICES AND ATTACHMENTS

As required by the assessment scope, the Evaluator shall provide a network, system or application diagram illustrating the information system architecture as an appendix to the IS Assessment Report. Other appropriate appendices include:

1. List of documentation provided and reviewed during testing;
2. CAP Management Worksheet;
3. CAP Review Worksheet;
4. The system or application test plan and test scripts when applicable;
5. Hardware and software inventories of exactly what was tested;
6. List of checks performed by automated vulnerability scanning software, particularly when few or no Business Risks have been documented; and
7. Screenshots demonstrating vulnerabilities documented within the report.

3.4.1. CAP MANAGEMENT WORKSHEET

The Business Owner shall prepare a CAP (Appendix C) for each open finding in the Final IS Assessment Report. To facilitate the CAP process, the Evaluator shall prepare a CAP Management Worksheet that records all findings identified during the assessment. Findings that are closed while the Evaluator is on-site, and that are verified as closed by the Evaluator, shall be noted as closed in the Final IS Assessment Report and are not included on the CAP Management Worksheet.

Ultimately, the information from the CAP Management Worksheet will be used by the Business Owner to populate the CMS Integrated Security Suite (CISS) Tool maintained by CMS. As described in the *CISS User Guide*, CMS uses the CISS Tool to track the status of open issues and findings.

The CAP Management Worksheet is part of the CMS POA&M Guidelines located at http://www.cms.hhs.gov/informationsecurity/downloads/poam_guidelines.pdf. These guidelines provide the templates and instructions for the completion of the CAP Management Worksheet. To support the mitigation efforts after the delivery of the final report, the Business Owner shall update the information provided in the CAP Management Worksheet in accordance with the CMS POA&M Guidelines.

3.4.2. CAP REVIEW WORKSHEET

The CAP Review Worksheet is a record of prior findings that the Evaluator may be tasked to review during the assessment. Appendix C contains the templates and instructions for the completion of the CAP Review Worksheet. The Evaluator shall prepare a CAP Review Worksheet to document the status of prior findings reviewed during the assessment. Prior findings are findings from previous ST&Es, assessments and audits.

4. DOCUMENTING BUSINESS RISKS

All vulnerabilities identified through the security assessment shall be presented in a manner that best conveys specific business risks to CMS. Each vulnerability will be documented as a finding that corresponds to at least one (1) control from one (1) of the seventeen (17) security control families identified in the *CMS PISP* or to the appropriate e-Authentication elements from *CMS IS ARS* Appendix A. The key objectives for the documentation of the business risks are to:

1. Identify which processes are not working effectively to safeguard information assets;
2. Describe the specific risks to the system's business functions and the CMS mission; and
3. Recommend methods to mitigate the residual risk to an organizationally acceptable level.

The primary audience for the findings, identified as Business Risks, includes Business Owners, System Developers / Maintainers, Administrators and other managers responsible for IS. Some members of the report audience, such as managers, may be concerned with the middle ground between an executive overview and technical details. Each Business Risk shall include mid-level metrics to describe the Risk Level, Ease-of-Fix and Estimated Work Effort. The Evaluator shall assess these metrics based upon the guidelines presented in this section.

4.1. FINDING NUMBER

The Evaluator, in accordance with the *CMS Finding Numbering Standards* (Appendix B), shall assign a number to each finding using the following instructions. Each section of digits of the numbering shall be separated by a dash. The format for the number is aaa(a)(a)-99-x(x)-999.

1. The first three, four or five characters are letters, which identify the name of the contractor or system.
 - a. For all external testing and data centers, each contractor is assigned a unique set of letters as listed in the CMS Office of Financial Management (OFM) *Medicare Financial Management Manual*, Chapter 7, Section 40.3, which is located at <http://www.cms.hhs.gov/manuals/downloads/fin106c07.pdf>. The CMS Medicare Contractor Management Group (MCMG), Division of Performance Assessment (DPA) maintains Section 40.3 of the *OFM Medicare Financial Management Manual*, and manages changes between the annual updates.
 - b. For internal systems, the CISS number assigned to the application is the identifier for the application. Contact Director, EASG or the CMS CISO if system information is not available.
2. The first two numeric characters are the last two numbers of the year of the review.
3. The third set of characters identify the type of review.

- a. One-character identifiers identify the type of review in accordance with the *OFM Medicare Financial Management Manual*, Chapter 7, Section 40.3 (see Appendix A or <http://www.cms.hhs.gov/manuals/downloads/fin106c07.pdf>).
 - b. Two-character identifiers identify types of reviews that are not included in the *OFM Medicare Financial Management Manual*. These are normally requirements based on other (non-financial) Federal security requirements.
4. The last three characters are sequential numbers which represent each individual finding (beginning with 001, 002, 003, etc.) for the year in review.

4.2. BUSINESS RISK STATEMENT

The Evaluator shall develop a brief statement summarizing the key point(s) of the finding description. This information should identify the key vulnerability concisely and the risk it presents to the system, the business function or to CMS. In the examples provided below, there is clear statement of the vulnerability, identification of the affected component or procedure, and the impact of the vulnerability upon the business function.

Examples:

INSUFFICIENT BACK-UP OF SYSTEM DATA MAY HINDER SUCCESSFUL RECOVERY FROM SYSTEM OUTAGES

EXCESSIVE DELAY IN REVOKING INACTIVE ACCOUNTS LEAVES CMS DATA VULNERABLE TO ABUSE

4.3. SECURITY CONTROL FAMILY

For all assessments, each finding should be associated with the security control families identified in the *CMS PISP*, *CMS IS ARS* or the e-Authentication requirements if applicable.

To categorize the business risks into security control families, the Evaluator shall identify the root cause of the vulnerability. The finding will be associated with the security control family related to the root cause, and to the corrective measures necessary to address the root cause. Other security control families may be associated with the same vulnerability, and the Evaluator shall evaluate whether the vulnerability, as it relates to other security control families, should constitute a separate finding. To the extent possible, each finding should relate to the vulnerability associated with the controls of one (1) security control family.

4.4. REFERENCES

The Evaluator shall identify the specific security controls that pertain to each finding. The control set used for reporting should correspond to the documented security control requirement specified within the scope of the assessment³.

Additionally, when reporting a technical finding, the Evaluator shall list any additional reference material that demonstrates the industry-standard or vendor-specific description of the vulnerability. This may include any of the following, or other requirement identifiers appropriate to the scope of the assessment:

- CMS Technical Reference Architecture or Supplemental Volumes;
- Department of Health and Human Services (DHHS) Configuration Baselines;
- Vendor knowledge base articles; and
- Common Vulnerability and Exposure (CVE) numbers that apply to the vulnerability.

For technical findings, the Evaluator shall obtain specific references from vulnerability scanning tools that report vendor or CVE information.

4.5. DETERMINATION GUIDELINES

The Evaluator shall determine the Risk Level and estimate the resources necessary to remediate the vulnerability identified in each finding. The Risk Level Determination Guidelines in this section follow those provided in NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*.

4.5.1. RISK LEVEL ASSESSMENT

The Evaluator shall consider the potential severity of the impact, the threat exposure, and the likelihood of occurrence to determine the Risk Level of the vulnerability (Low, Moderate or High) identified in the finding. The Risk Level summarizes the overall level of risk the vulnerability presents to the information system.

The Likelihood of Occurrence indicator for each Threat Exposure is not an absolute and should be considered within the context of the information system being evaluated. The Likelihood of Occurrence classifications are defined in Table 2 below.

Table 2: Likelihood of Occurrence Classifications

³ The Document Security Control Requirement is defined in the scope statement. Refer to *CMS IS Assessment Procedure*, Section 2.2, Initiation of the Assessment Planning Phase for more information.

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

The Threat Exposure shall be classified based on the descriptions provided in Table 3 below. If more than one Threat Exposure applies to a particular vulnerability, the one representing the greatest level of exposure as determined by the Evaluator or is this the last item in the table or based on the user community or something else shall be used.

Table 3: Threat Exposure Classifications, including Likelihood of Occurrence

Threat Exposure	Description and Likelihood of Occurrence
Procedural	Threat exposures that are non-human factors. Lack of Disaster Recovery Plans, weak password policies, and poor back-up policies are examples of procedural threat exposures. The Likelihood of Occurrence for vulnerability exploitation is Low.
Authorized Internal User	A user who has been granted access to the CMS system affected by the vulnerability. A CMS employee, Business Partner, or a third-party contractor who has been granted access to CMS systems. The Likelihood of Occurrence for vulnerability exploitation is generally Low.
Unauthorized Internal User	A user who has access to a CMS facility and CMS systems, but has not been granted access to the system or system functions

Threat Exposure	Description and Likelihood of Occurrence
	<p>affected by the vulnerability.</p> <p>This may be a CMS employee, Business Partner or third-party contractor who has been granted access to CMS systems. An Unauthorized Internal User may also be a visitor who has access to a CMS facility and, therefore, physical access to the CMS network.</p> <p>The Likelihood of Occurrence for vulnerability exploitation is Moderate.</p>
Authorized External User	<p>This may be a CMS employee, Business Partner, third-party contractor or vendor technician working from an off-site location with access to the CMS network through a dial-up line, a virtual private network (VPN) connection, or through an AT&T Global Network Service (AGNS) connection.</p> <p>The Likelihood of Occurrence for vulnerability exploitation is Low.</p>
Unauthorized External User	<p>This is any off-site individual who attempts to access CMS information systems without the use of access privileges. This includes individuals who may attempt to access the CMS network using a dial-up line, a VPN connection, or the AGNS network.</p> <p>The Likelihood of Occurrence for vulnerability exploitation is Moderate.</p>
Authorized Internet User	<p>This includes any individual who has been authorized to access a CMS web-based application (e.g. QualityNet) that is available over the Internet. The community of users may include Providers, Physicians and other data vendors.</p> <p>The Likelihood of Occurrence for vulnerability exploitation is Moderate.</p>
Unauthorized Internet User	<p>A user who can connect to public CMS systems, but is not authorized to access Internet-accessible CMS applications. This includes any individual in the general Internet population who may access a CMS-hosted web page.</p> <p>Based on the number of potential users, the Likelihood of Occurrence for vulnerability exploitation is High.</p>

Threat Exposure	Description and Likelihood of Occurrence

Impact severity of an exploited vulnerability shall be assessed based on the categories in Table 4 below. Each category describes the potential effects of the exploited vulnerability to the confidentiality, integrity and availability of information processed, stored or transmitted by the information system being evaluated.

Table 2: Impact Severity Classifications

Impact Severity Classification	Description
Critical	A CMS core business function is disabled indefinitely. The integrity or availability of mission critical information is compromised. The disclosure of defense, intelligence or national security information would have a critical impact severity if CMS possessed any such information.
Severe	Information protected by the Privacy Act of 1974 or other CMS sensitive but unclassified information is disclosed. The confidentiality and integrity of sensitive information is compromised. Important information services may be rendered unavailable for an extended period of time.
Serious	The integrity of non-sensitive, non-critical information is compromised (for example, a web page is altered giving false information that misleads CMS beneficiaries). Availability of a critical information system(s) may also be compromised for a limited time, but no sensitive information is disclosed.
Significant	The inability of the CMS public user community to access a CMS information system(s) for a limited time, rendering the service(s) inoperable to its primary users.

Impact Severity Classification	Description
Minor	A minor impact indicates a temporary effect on the availability of non-critical information (e.g., an Internet Control Message Protocol (ICMP) Denial-of-Service attack on a web server). No sensitive information is disclosed, and the integrity of information is preserved.

Table 5 below provides a matrix that pairs the Threat Exposure with the Impact Severity Classification (ISC) to identify the resulting Risk Level.

Table 3: Risk Level Classifications

Threat Exposure	ISC Minor	ISC Significant	ISC Serious	ISC Severe	ISC Critical
Procedural	Low	Low	Moderate	Moderate	High
Authorized Internal User	Low	Low	Low	Moderate	High
Unauthorized Internal User	Low	Low	Moderate	High	High
Authorized External User	Low	Moderate	Moderate	High	High
Unauthorized External User	Moderate	Moderate	High	High	High
Authorized Internet User	Moderate	Moderate	High	High	High
Unauthorized Internet User	High	High	High	High	High

The assigned Risk Level for the vulnerability shall be described in the assessment report using the definitions provided in Table 6 below.

Table 4: Risk Level Definitions

Rating	Definition of Risk Rating
High Risk	Exploitation of the technical or procedural vulnerability will

Rating	Definition of Risk Rating
	cause substantial harm to CMS business processes. Significant political, financial and legal damage is likely to result.
Moderate Risk	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS.
Low Risk	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment.

4.5.2. EASE-OF-FIX ASSESSMENT

The Evaluator shall assign an Ease-of-Fix rating based on an estimation of the relative complexity required to reduce, eliminate or otherwise mitigate the Business Risk. The assessment shall be described using the guidelines in Table 7 below.

Table 5: Ease-of-Fix Assessment

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data.

Rating	Definition of Ease-of-Fix Rating
<p>Moderately Difficult</p>	<p>Remediation efforts will likely cause a noticeable service disruption.</p> <ul style="list-style-type: none"> • A vendor patch or major configuration change may be required to close the vulnerability. • An upgrade to a different version of the software may be required to address the impact severity. • The system may require a reconfiguration to mitigate the threat exposure. • Corrective action may require construction or significant alterations to the manner in which business is undertaken.
<p>Very Difficult</p>	<p>The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling.</p> <ul style="list-style-type: none"> • An obscure, hard-to-find vendor patch may be required to close the vulnerability. • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity. • Corrective action requires major construction or redesign of an entire business process.
<p>No Known Fix</p>	<p>No known solution to the problem currently exists. The Risk may require the Business Owner to:</p> <ul style="list-style-type: none"> • Discontinue use of the software or protocol. • Isolate the information system within the enterprise, thereby eliminating reliance on the system. <p>In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by CMS IS Management, to validate that security incidents have not occurred.</p>

4.5.3. ESTIMATED WORK EFFORT ASSESSMENT

The Evaluator shall assign an Estimated Work Effort rating based on an estimation of the time commitment required for CMS or contractor personnel to implement an appropriate remediation for the business risk. The assessment shall be categorized based on Table 8 below.

Table 6: Estimated Work Effort Rating

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective actions.
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions.
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units.
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

4.6. BUSINESS RISK DESCRIPTION

Complete the “Description” section of the Business Risk template by documenting the details of the vulnerability. Document whether the weaknesses were discovered through an interview, document review or the use of a testing tool.

4.6.1. TECHNICAL FINDING

Technical findings will contain system-specific information about the weakness, including CVE numbers and citations to other sources for information about a reported vulnerability. Technical findings relate vulnerabilities that may lead directly to an exposure of information assets.

Complete the “Description” section of the Business Risk template by documenting the technical details of the vulnerability, which include:

1. How the vulnerability was discovered and validated;
2. How the vulnerability could be exploited;
3. Who may exploit the vulnerability;
4. What systems (IP addresses) are affected by the vulnerability; and
5. The harm or damage that would occur if the vulnerability were to be exploited.

The harm or damage that may occur if the vulnerability were to be exploited shall be described in terms of the business impact to CMS. Specifically, how the confidentiality, integrity and availability of information may be affected and what type and sensitivity level of information is at risk of compromise.

4.6.2. PROCEDURAL FINDING

A procedural finding indicates a weakness in the policies and processes that are in place to protect the system. Generally, procedural findings relate vulnerabilities that will not lead directly to the compromise of information assets.

Complete the “Description” section of the Business Risk template by documenting the details of the vulnerability, which include:

1. How the vulnerability was discovered and validated;
2. The relationship of the vulnerability to the control requirements (there is no need to restate the requirement cited in “References” section);
3. How the vulnerability could be exploited;
4. Who may exploit the vulnerability;
5. What business functions are affected by the vulnerability; and
6. The residual risk to CMS if the Business Owner fails to mitigate the vulnerability.

The residual risk that may remain if the vulnerability is not mitigated shall be described in terms of the business impact to CMS. Specifically, how the confidentiality, integrity and availability of information assets may be affected.

4.7. SUGGESTED CORRECTIVE ACTIONS

Complete the “Suggested Corrective Actions” section of the Business Risk template by documenting the remediation procedures necessary to close or reduce the vulnerability. Remediation procedures may include, but are not limited to, applying patches or service packs, upgrading hardware or software, implementing new or different controls, modifying configuration settings, or developing or modifying information security policy.

The Evaluator, in developing the Suggested Correction Actions for a finding, shall consider available CMS and Business Partner resources, provide a suitable level of technical information, and address the risks identified in the “Description” section. The procedures indicated in the “Suggested Corrective Actions” section shall be presented in a step-by-step, sequentially-numbered, multi-level outline format. The “Suggested Correction Actions” section should also

address any residual risks that may remain after the procedures are followed to ensure that additional vulnerabilities that may expose CMS systems are not introduced.

4.8. STATUS

The Evaluator shall identify in the “Status” section the date the Business Risk was first identified. The Evaluator shall record any subsequent actions, or discussion of the finding, by CMS, contractors or other parties to the assessment, as a comment. Comments are used by the Evaluator to convey the discussion of the finding between all parties involved. The Evaluator may include comments from the Business Owner, the Facilitator or from other members of the evaluation team to help convey any issues related to the finding. Examples of subsequent actions to include in the “Status” section include, but are not limited to, closing or reducing the impact of the vulnerability by completing corrective actions, providing sufficient evidence to show that the vulnerability no longer exists, or performing validation testing to verify that the vulnerability no longer exists.

If additional documentation is reviewed after the original assessment, the Evaluator shall be expected to state clearly, what documentation was received, why additional documentation was provided, and a brief analysis of the received documentation to explain how it relates to the remediation of the finding.

The Evaluator may indicate whether the information provided during or after testing may be sufficient to close the finding. The Evaluator shall provide a recommendation that the finding be closed based on an evaluation of the information provided after the vulnerability was identified. Final closure of the finding is at the discretion of CMS Management.

5. SECURITY ASSESSMENT REPORT PACKAGE

After the completion of the assessment report, the Evaluator shall prepare an IS Assessment Report Package and deliver the package to the Facilitator. There are two versions of the IS Assessment Report Package:

- 1) Final Report Package: Contains the Final IS Assessment Report; the CAP Management Worksheet, and its instructions, that the Facilitator shall provide to the Business Owner, and other responsible parties; and the CAP Review Worksheet, if a CAP review was conducted; and
- 2) Final Book Package: Contains the contents of the Final Report Package and includes all of the working papers and supporting materials for the assessment that the Facilitator will provide to the Business Owner.

All deliverables become the property of the CMS CIO. The Evaluator shall maintain electronic copies of all materials contained within the Final Report Package and the Final Book Package for three (3) years, in accordance with National Archives & Records Administration (NARA) General Records Schedule 24, April 2003.

In accordance with provisions within the Paperwork Reduction Act (44 CFR 35), the contents of the Final Book Package shall be provided in an electronic format, as specified below in Section 5.3. Security for the electronic files, and the delivered media containing the electronic files, shall be in accordance with section 5.3.1 as well as the Media Protection controls as defined in the *CMS PISP* and the *CMS IS ARS*.

5.1. FINAL REPORT PACKAGE

The Evaluator shall include the following documents below as attachments within the Final Report Package:

1. Final IS Assessment Report (.doc)
2. Final IS Assessment Report (.pdf)
3. CAP Management Worksheet (.xls)
4. CAP Management Instruction Sheet (.doc)
5. CAP Review Worksheet (.xls)

All electronic documents must be Section 508 compliant.

The Evaluator shall deliver the Final Report Package to the Facilitator in encrypted electronic format and in hardcopy format in a three-ring binder. The Facilitator shall be responsible for providing the Final Report Package documents directly to the Business Owner.

5.2. FINAL BOOK PACKAGE

The Final Book Package contains the official copy of the assessment records, including all original working papers, notes and scripts. The Evaluator shall deliver, to the Facilitator, the official CMS records of the assessment, including all original documents, working papers, notes, and communications related to the assessment. The Evaluator shall package original records in a clearly labeled three-ring binder with tabbed sections for the contents defined in the following list:

1. Letter of Introduction
2. Scope
3. Test Plan
4. Final IS Assessment Report (.doc)
5. Final IS Assessment Report (.pdf)
6. CAP Management Worksheet (.xls)
7. CAP Management Instruction Sheet (.doc)
8. CAP Review Worksheet (.xls)
9. Documentation
10. Test Script
11. Working Papers

The Evaluator shall prepare a CD containing the contents of the Final Book Package in an electronic format. All electronic documents must be Section 508 compliant. The folder structure of the media shall conform to the labels of the tabbed sections provided above. The media containing the assessment files shall be provided to the Facilitator with the Final Book Package.

The Facilitator shall disseminate the contents of the Final Book Package to the Business Owner. The CMS CIO, or the CMS CISO may use the contents of the Final Book Package to support other agency audit activities.

5.2.1. COMMUNICATIONS

The Communications section of the Final Book Package contains the documented communications between the assessing entity and CMS throughout the security assessment. The type of communications to be included, but are not limited to:

1. E-mails
2. Meeting agendas
3. Meeting minutes and notes
4. Voice messages
5. Facsimiles
6. Letters
7. Delivery courier receipts

In the instances of electronic communications resulting in file or printing format, the communication shall be printed in its original, unaltered state. If an e-mail displays replies to the original e-mail then the e-mail containing the most replies may be printed instead of reprinting each individual e-mail separately, as long as all communications are captured in connection with the originating e-mail.

Where technology permits, voice-mail messages may be stored as electronic audio files. Any audio files retained for the Final Book Package must be in a format supported by the CMS Desktop baseline configuration (i.e. “MP3” or “WMA” format). The filename shall indicate the date and time of the communication, as well as the name and organization of the individuals both sending and receiving the message.

5.2.2. WORKING PAPERS

The Evaluator shall document the activities of the assessment, from the beginning of the security assessment process to the Final IS Assessment Report, in a collection of working papers.

Working papers contain evidence accumulated during the assessment which demonstrates what tests were performed, the results of the assessment procedures, the analysis of the data collected, the vulnerabilities identified and the conclusion of the Evaluator. Working papers shall be retained as hard copy documents, but will also need to be converted to an electronic format for delivery.

The Evaluator may record additional notes during the assessment. Notations may demonstrate the validation of information provided by automated scanning tools, may provide a transcript of an interview, or otherwise reflect the analysis of reviewed documents. The notes taken for technical testing may also address the elimination of false-positives or identify additional vulnerabilities to investigate. These notations, whether related to technical tests, interviews, or supporting documentation, will be provided in their original format, and in an electronic format, in the working papers.

Items that may be included as working papers include, but are not limited to:

1. Review programs
2. Results of specialized programmatic scripts or automated tools and scans
3. Personal Notations
4. Interview transcripts
5. Analyses
6. Memoranda
7. Letters of confirmation and representation
8. Abstracts of documents
9. Schedules
10. Commentaries prepared or obtained by the reviewer

The following abstract is from the CMS *Medicare Financial Management Manual*, Chapter 7, §20.5, includes additional Working Paper production guidance, as provided below:

General Content of Working papers

Working papers should ordinarily include documentation showing that:

- The work has been adequately planned and supervised
- The review evidence obtained, the reviewing procedures applied, and the testing performed has provided sufficient, competent evidential matter to support the reviewer's judgments and/or conclusions

Format of Working Papers

Working paper requirements should ensure that the working papers follow certain standards. As a whole, a good set of working papers should contain the following:

- The objectives, scope, methodology and the results of the review
- Proper support for findings, judgments and/or conclusions, and to document the nature and scope of the work conducted
- Sufficient information so that supplementary oral explanations are not required
- Adequate indexing and cross-referencing, and summaries and lead schedules, as appropriate
- Date and signature by the preparer and reviewer
- Evidence of supervisory review of the work
- Proper heading should be given to the basic content of the working papers

Also included within the Working Papers section are written responses, questions or notations by the Business Owner, System Developer / Maintainer, or other Facilitator contact, in the presence of the Evaluator.

5.2.3. DOCUMENTATION

Any documents released to the Evaluator by the Facilitator shall be included in this section of the Final Book Package. This includes documentation received during any phase of the assessment process.

During the assessment-planning phase, the Evaluator shall receive system documentation from the Facilitator and the Business Owner. The received documentation provides information critical to the development of the test plan, the scope, and the resource planning of the assessment. Received documents may include, but are not limited to:

1. SSP
2. IS Risk Assessment
3. Contingency Plan
4. System or network diagrams
5. System names and locations
6. Contact information
7. System configuration documentation

During the assessment, the Evaluator may use vulnerability and scanning tools, or other assessment utilities, which generate reports. The analysis of the generated reports provides the information necessary to identify any system vulnerabilities. The generated reports may be quite lengthy and should be provided in an electronic format. System-related staff, during interviews with the Evaluator, may identify other documents to support the assessment process. All of the identified documents, once provided to the Evaluator by the Facilitator shall be included. Information that the Business Owner did not release for delivery to the Evaluator, but was reviewed by the Evaluator during the assessment, should be listed in the Final IS Assessment Report with the name, version and date of the documents.

As the Evaluator prepares the draft IS Assessment Report, and until the discussion of the draft report is held, the Business Owner may provide additional documentation to support or refute a finding, or to demonstrate that a CAP is being developed. In this instance, the Business Owner shall provide the documented evidence of the remediation through the Facilitator to the Evaluator. The Evaluator shall have five (5) business days following the draft report discussion to finalize the report.

The Evaluator shall provide a complete index of all documents used to support the assessment as an appendix to the Final Book Package.

5.3. DELIVERABLE FORMATTING

To preserve the integrity of files provided as a Microsoft Word (.doc) file, the Evaluator shall configure the Final IS Assessment Report as a password-protected “Read-only” file. The Microsoft Excel (.xls) file for the CAP Management and CAP Review Worksheets shall also be protected as “Read-only” files as the sensitivity of the information requires.

All media transferred between the Evaluator and the Facilitator shall be labeled in accordance with the standards provided by the *CMS PISP* and the *CMS IS ARS*.

A password-protected CD-ROM shall be created as part of the Final Report Package and Final Book Package. The CD-ROM shall contain the report in electronic format, the Findings Tracking form, the Weakness Summary report, and the POA&M Form. The CMS official copy CD-ROM will also contain all working papers produced, created or stored in electronic format.

Electronic files may be delivered between the Facilitator and the Evaluator via e-mail. All files shall be encrypted and password-protected in accordance with the *CMS PISP*.

Passwords shall be sent in a separate transmission for security purpose.

APPENDIX A: CMS IS FINDINGS REPORT TEMPLATE

The CMS IS Findings Report Templates can be found located at <http://www.cms.hhs.gov/informationsecurity>

How To Use The Templates

Document Section	Description
Boilerplate	<p><i>Boilerplate</i> language that shall be used in all reports is included in applicable sections. In other sections, the information must be entered based upon the individual circumstances of each assessment. The language that must be changed for each report is included within {brackets}, and is highlighted in gray.</p> <p>Other sections include <i>Sample</i> language recommended for use in all reports, but will vary depending on the system under review. The difference between boilerplate language and sample language are defined within the Important: annotations in the template. Language that must be removed from the final document is highlighted in yellow.</p>
Cover Page	The Cover Page contains boilerplate information that shall be included within all reports.
Section 1	Section 1, Executive Summary, contain both sample language and boilerplate language. This section contains instructions for the types of information that shall be included within the Executive Summary.
Section 2	Section 2, Introduction, contains sample language that shall be used when appropriate. Based upon the circumstances of the assessment engagement, the Evaluator shall supplement or modify the sample language.
Section 3.0	Section 3.0, Detailed Findings, contains boilerplate language that shall be included within all reports.
Section 3.1	Section 3.1, Procedure for Security Assessment, contains sample language that shall be used in all

Document Section	Description
	reports, where appropriate. This language, however, will change based upon the scope of the assessment and assessment procedures.
Section 3.2	Section 3.2, Procedure for Security Assessment Reporting, contains boilerplate language that shall be included within all reports.
Sections 3.3, 3.4, 3.5 and 3.6	Sections 3.3, 3.4, 3.5 and 3.6 are the detailed business risk findings and contain boilerplate language that should be included within all reports.

APPENDIX B: CMS FINDINGS NUMBERING STANDARD

The standards used to identify and enumerate the findings within a report are subject to federal mandates and guidance, as listed in part, in the CMS Office of Financial Management (OFM) *Medicare Financial Management Manual*, Chapter 7, Section 40.3.

In addition to the format of the report following a strict template (either the *CMS IS Findings Report Template for Applications* or the *CMS IS Findings Report Template for Business Partner Sites / Infrastructure*), each finding within the report shall be numbered in a specific manner to identify the contractor, the year of the test, and the type of test / review. This numbering standard will allow CMS to track findings, utilizing various tools without the risk of duplication or the loss of tracked findings.

Findings Numbering Process

The Evaluator shall assign a number to each finding using the following instructions. Each section of digits of the numbering shall be separated by a dash. The format for the number is aaa(a)(a)-99-x(x)-999.

1. The first three, four or five characters are letters, which identify the name of the contractor or system.
 - a. For all external testing and data centers, each contractor is assigned a unique set of letters as listed in the CMS Office of Financial Management (OFM) *Medicare Financial Management Manual*, Chapter 7, Section 40.3, which is located at <http://www.cms.hhs.gov/manuals/downloads/fin106c07.pdf>. The CMS Medicare Contractor Management Group (MCMG), Division of Performance Assessment (DPA) maintains Section 40.3 of the *OFM Medicare Financial Management Manual*, and manages changes between the annual updates.
 - b. For internal systems, the CISS number assigned to the application is the identifier for the application. Contact Director, EASG or the CMS CISO if system information is not available.
2. The first two numeric characters are the last two numbers of the year of the review.
3. The third set of characters identify the type of review.
 - a. One-character identifiers identify the type of review in accordance with the *OFM Medicare Financial Management Manual*, Chapter 7, Section 40.3 (see Appendix A or <http://www.cms.hhs.gov/manuals/downloads/fin106c07.pdf>).
 - b. Two-character identifiers identify types of reviews that are not included in the *OFM Medicare Financial Management Manual*. These are normally requirements based on other (non-financial) Federal security requirements.
4. The last three characters are sequential numbers which represent each individual finding (beginning with 001, 002, 003, etc.) for the year in review.

Review Type Identifiers

Identifier	Types of Review
<i>In accordance with OFM Financial Manual, Chapter 7</i>	
R	Accounts Receivable review
C	CPIC (the annual self-certification package)
E	CFO EDP review
F	CFO Financial review
S	Statement on Auditing Standards number 70 (SAS70)
O	OIG reviews (HHS Office of Inspector General (Information Technology) controls assessment)
G	Government Accountability Office (GAO) reviews (financial reviews)
P	CMS 1522 workgroups reviews
V	CFO related NVA/ST
N	SAS 70 Novation
M	CMS CPIC workgroup reviews
<i>Not included in the OFM Financial Manual</i>	
9T	Section 912 testing
9E	Section 912 Evaluations
AC	CMS Self-assessment Annual Compliance Audits
IR	Internal reviews initiated by the entity to meet other federal requirements
RA	Issues identified during routing risk assessments

- The last three digits are numbers assigned to each individual finding (beginning with 001, 002, 003, etc.), for the year of the review.

Examples of material weaknesses reported in a Corrective Action Plan (CAP) or Plans of Action and Milestones (POA&M) over three years would be:

- NGS-07-C-001;
- NGS-07-C-002;
- CIG-04-9T-003;
- NGS-06-9E-001;
- PGBA-07-9E-002;
- HLN-06-IR-002; and
- HLN-06-RA-001.

NOTE: While reporting on applications, entities and/or systems, a type of review or an entity that is not represented within the lists above may need to be created. In this case, the tester or Medicare Contractor shall contact CMS for the appropriate numbering standard (acronyms or identifiers).

APPENDIX C: CAP MANAGEMENT

CAP Management is an integral part of the CMS security program and a federal requirement. Tracking the CAPs to closure is also an important piece of the Systems Development Life Cycle (SDLC) of any system and plays a large part in the vulnerability assessment and reporting process. Federal Information Security Management Act (FISMA) reporting requirements exist for most federal systems and the following forms are critical in ensuring compliance and proper risk mitigation and closure procedures are followed.

Instructions for CAP Management Worksheet

The following instructions explain how the CAP Management Worksheet shall be completed. This is an integral part of the reporting process and assists CMS and the Business Owner with FISMA compliance. The initial update to the form will require more information than the monthly updates / status reports. Information must be entered in columns 1, 2, 3, 4, 5, 6, 8, 9 and 10 for each reported finding / action item for the initial submission. Once the initial CAP Management Worksheet has been completed and submitted to OIS- Enterprise Architecture and Strategy Group, no changes may be made to the data in columns 1, 2, 3, 4, 5, 6, and 8. Only columns 7, 9, 10 and 11 may be updated for the monthly reporting. When a finding / action item is closed, either during the initial or monthly submission, specific documentation for verification is required along with the submission.

For sites / General Support Systems (GSSs) / applications that are subject to FISMA reporting requirements, this CAP Management Worksheet will be used to generate the POA&M that is updated and submitted quarterly to the Department.

Column 1 -Tracking Number. This column is for the tracking number that is assigned to the weakness when entering the weakness into the CMS Integrated Security Suite (CISS) Tool.

Column 2 -Weakness. The description of the detailed finding / action item identified in an Authority to Operate (ATO) or C&A memorandum will be pre-filled in this column. Sensitive descriptions of specific findings are not necessary, but sufficient data must be provided to permit oversight and tracking. **Example of a Weakness: The System's System Security Plan (SSP) and Risk Assessment (RA) are out-of-date.**

Column 3 – POC. Identify the name of the Point of Contact (POC), position / title and organizational entity that the component head will hold responsible for resolving the finding and/or action item. **Must be a CMS staff.**

Column 4 – Resources Required. Identify the estimated staff time, in hours, required to resolve the finding and/or action item. Identify any cost (e.g. contract costs) associated with resolving the finding and/or action item and identify the Financial Management Investment Board (FMIB) number for the investment. This column cannot be left blank or equal 0.

Column 5 – Scheduled Completion Date. Identify the scheduled completion date (mm/dd/yy) for resolving all the milestones associated with the finding / action item. Please note that the

initial date entered may not be changed. If a finding / action item is resolved before or after the originally scheduled completion date, the CMS Business Owner [or designee] should note the actual completion date in Column 9, "Completion Date." EASG recommends the following four dates as the scheduled completion dates for Column 5: January 2, 20xx, April 2, 20xx, July 2, 20xx or October 2, 20xx.

Column 6 – Milestone Completion Dates. Key milestones with completion dates must be entered into this column. A milestone will identify specific requirements or key steps to correct an identified finding / action item. If the finding / action item has two or more identified issues or elements contributing to the overall finding / action item, the milestones and completion dates must be comprehensive enough to address all elements of the finding / action item. Please note that after the CAP Management Worksheet milestones and completion dates are entered into the CISS tool, they cannot be changed. Any changes to the initial milestones or completion dates should be noted in column 7, "Changes to Milestones" with the necessitating reason in column 11 "Comments." An example of Milestones would be: Milestone 1: Update System's SSP
Milestone 2: Update System's RA.

Column 7 – Changes to Milestones. Complete this column only if the CAP cannot be completed by the Milestones Completion Date from Column 6 or the Scheduled Completion Date in Column 4 cannot be met. This column would include new completion dates for particular milestones or scheduled completion date. The reason for the change must be recorded in Column 11 "Comments."

Column 8 – Identified. The source of where the finding / action item was found and the associated finding numbers are entered in this column. Example: ATO-001, 2006 CFO Audit-005.

Column 9 – Completion Date. The date that all the milestones have been completed.

Column 10 – Status. The only entries permitted are "on-going", "delayed" or "completed." If "delayed", an entry must be made in Column 7 "Changes to Milestones" with new completion dates for the particular milestone. The reason for the change must be recorded in Column 11, "Comments".

Column 11 – Comments. Record a brief summary of the work accomplished during the reporting period. An entry is also required if a scheduled completion date or milestones date is missed (record the reason) or if the finding / action item has been corrected and all work is deemed "completed" (record the date of completion). Record any additional details or clarification for any previous entries as well as the application / system name related to the finding in this field.

Column 12 – Risk Level. This is the risk level [High, Moderate, or Low] assigned to the finding by the reviewer and cannot be changed by the Business Owner or System Developer / Maintainer. Any findings without a designated Risk Level will be assigned by EASG.

Column 13 –Weakness Severity. The severity level is "Weakness".

CAP Management Worksheet

1	2	3	4	5	6	7	8	9	10	11	12	13
Tracking #	Weakness	POC (CMS Staff)	Resources (Hours or Dollars)	Scheduled Completion Date	Milestone Completion Date	Changes to Milestones	Identified	Completion Date	Status	Comments	Risk Level	Weakness Severity

For further guidance and instruction for the purpose and procedures surrounding the CAP Management Worksheet or the POA&M, refer to the *CMS Plan of Action & Milestones (POA&M) Guidelines* located on the Internet at http://www.cms.hhs.gov/informationsecurity/downloads/poam_guidelines.pdf.

Instructions for CAP Review Worksheet

The following instructions explain how the Corrective Action Plan (CAP) Review Worksheet should be completed. This is an integral part of the testing and reporting process and assists CMS and the business owner with FISMA compliance. Information must be entered in every column for each reported finding before submission. Once the initial CAP Review Worksheet has been completed and submitted to the Facilitator, no changes may be made to the data in columns 1, 2 and 3. Only columns 6, 8, 9 may be updated for the monthly reporting. When a finding is closed, either during the initial or monthly submission, specific documentation for verification is required along with the submission.

For {sites/ GSSs /applications} that are subject to FISMA reporting requirements, this CAP Review Worksheet will be used by the Evaluator to confirm information recorded within the POA&M which is updated and submitted quarterly to the DHHS through the CISS tool. Further guidance and instruction for CISS or the POA&M process can be obtained through the *CMS Plan of Action & Milestones (POA&M) Guidelines* located through the CMS Information Security website:
http://www.cms.hhs.gov/informationsecurity/downloads/poam_guidelines.pdf.

Column 1 –Weakness. The description of the detailed finding identified in the {*SITE/ GSS /Application (acronym)*} {*type of test*} *Findings Report* will be pre-filled in this column. Sensitive descriptions of specific findings are not necessary, but sufficient data must be provided to permit oversight and tracking.

Column 2 –Finding ID. The number assigned to the finding within the {*SITE/ GSS Application (acronym)*} {*type of test*} *Findings Report* will be pre-filled in this column. This number is also the tracking number that is assigned to the weakness when entering the weakness into CISS Tool.

Column 3 –POC. Identify the name of the Point of Contact, position / title and organizational entity that the component head holds responsible, for resolving the finding.

Column 4 – Status. The only entries permitted are “Open” or “Closed”. An entry must be made in column 5, and the reason recorded in column 6. In addition, the completion date must be entered in column 6.

Column 5 – Supporting Documentation. Record a list of the documentation provided to support / justify the recorded Status. An entry is also required if the Status differs from the CAP Management Worksheet.

Column 6 - Comments. Record a brief summary of the assessment of the CAP and justification, in the perspective of the Evaluator, for the reported Status. An entry is also required if any differences exist between the CAP Management Worksheet and the CAP Review Worksheet.

CAP Review Worksheet

Subject of Review:
[Contractor]
Reviewer:

Date Rec'v'd by Facilitator:
Date Received by
[Contractor]:
Return Date to Facilitator:

1	2	3	4	5	6
Weakness	Findings ID	POC	Status	Supporting Documentation	Comments

APPENDIX D: RESOURCES & REFERENCES

- *Federal Information Security Management Act (FISMA) of 2002, PL 107-347.*
- Government Accountability Office (GAO), *Federal Information Systems Controls Audit Manual (FISCAM)*, GAO/AIMD-12.19.6, January 1999.
- Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003
- OMB, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-07-09, July 2007
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-42, *Guideline on Network Security Testing*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 3
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Third Public Draft
- NIST SP 800-63, *Electronic Authentication Guideline*, Version 1.0.1
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- NIST Interagency Report (IR) 7328, *Security Assessment Provider Requirements and Customer Responsibilities*, Initial Public Draft
- NIST IR 7359, *Information Security Guide For Government Executives*
- NIST Federal Information Processing Standards (FIPS) 191, *Guideline for the Analysis of Local Area Network Security*
- *Centers for Medicare & Medicaid Services (CMS) Information Security Virtual Handbook*, <http://www.cms.hhs.gov/informationsecurity>
- National Archives and Records Administration, *General Records Schedule 27, Records of the Chief Information Officer*, Transmittal 14, April 2005

APPENDIX E: ACRONYMS

ARS	Acceptable Risk Safeguards
ASP	Active Server Page
AGNS	AT&T Global Network Service
BPSSM	Business Partner System Security Manual
C&A	Certification & Accreditation
CAP	Corrective Action Plan
CIA	Confidentiality Integrity and Availability
CIG	Cigna Healthcare
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISS	CMS Integrated Security Suite
CMS	Centers for Medicare and Medicaid Services
CMSR	CMS Minimum Security Requirements
CVE	Common Vulnerability and Exposure
DHHS	Department of Health and Human Services
EASG	Enterprise Architecture and Strategy Group
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FMIB	Financial Management Investment Board
GAO	Government Accountability Office
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HLN	Healthnow New York, Inc
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IR	Interagency Report
IRS	Internal Revenue Service
IS	Information Security
ISC	Impact Severity Classification
ISSO	Information System Security Officer
MA	Major Application
MDCN	Medicare Data Communications Network
MP3	Moving Picture Experts Group -1 Audio Layer 3
NGS	National Government Services
NIST	National Institute of Standards and Technology
OFM	Office of Financial Management
OIG	Office of Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PISP	Policy for the Information Security Program
POA&M	Plan of Action & Milestones
RA	Risk Assessment

RoE	Rules of Engagement
SAS	Statement on Auditing Standards
SDLC	System Development Life Cycle
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
ST&E	Security Test & Evaluation
VPN	Virtual Private Network
WMA	Windows Media Audio

End of Document