Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Procedure:

POA&M and Annual FISMA Assessment Using CISS

FINAL
Version 1.0
March 19, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *POA&M AND ANNUAL FISMA ASSESSMENT USING CISS*, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 PURPOSE

This document provides the procedures necessary for the Centers for Medicare & Medicaid Services (CMS) to complete and submit Plan of Action and Milestones (POA&M) and annual Federal Information Security Management Act of 2002 (FISMA) assessment using the CMS Integrated Security Suite (CISS) application.

This document is the former Appendix A to the *CMS Business Partners Systems Security Manual (BPSSM)*. The former BPSSM Appendix A Core Security Requirements (CSRs) Attachments 1, 2, and 3 are now included in the new *CMS Information Security Acceptable Risk Safeguards (ARS) Including Minimum Security Requirements* (CMSRs) document as Appendix A (*CMSR High Impact Level Data*), Appendix B (*CMSR Moderate Impact Level Data*), and Appendix C (*CMSR Low Impact Level Data*), respectively.

2 SCOPE

Unless otherwise directed by CMS, this document applies to all CMS Business Owners and System Developers/Maintainers. This includes all CMS internal/external business entities including their contractors/subcontractors, and organizational employees and facilities that support CMS business missions. All of these business organizations are referred to as “entities” in this document.

The procedures provided in this document refer to processes and/or inputs that apply primarily to the CISS application security elements, forms, and/or form fields. Readers of this document should be familiar with the CISS application or refer to the *CISS User Guide* to better understand the procedures documented here. The *CISS User Guide* is included within CISS as a help file and on the CMS Information Security Library Web page: http://www.cms.hhs.gov/InformationSecurity/ISD/list.asp.

3 BACKGROUND

CMS is required to track and report ongoing security issues and corrective action status information in response to federal statutes, such as FISMA. FISMA requires that federal agencies provide annual reporting on the state of security programs for all information technology (IT) systems associated with the agency. Additionally, the Office of Management and Budget (OMB) requires that all federal agencies report the status of known security weaknesses for all agency systems in periodic POA&Ms. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under Federal Manager’s Financial Integrity Act of 1982 [FMFIA]). In the case of FISMA, any security weakness identified for covered systems shall be reported and included in periodic (e.g., monthly or quarterly) POA&M reports.

POA&M and Annual FISMA Assessment Using CISS

A critical factor for maintaining on-going compliance with federal requirements is for CMS Business Owners, in coordination with system and application developers/maintainers, to annually test their internal controls. To meet the FISMA aspect of this requirement, they are required to schedule and perform a FISMA annual security control assessment; and oversee the development and completion of applicable POA&Ms for vulnerabilities (i.e., findings) noted during the annual FISMA Assessment (FA).

4 CMS INTEGRATED SECURITY SUITE (CISS)

The CISS (pronounced "kiss") allows CMS management and entities to track ongoing security issues and status information, as well as meet the FISMA POA&M and FA reporting requirement for all security-related findings. The CISS operating procedures are provided in the *CISS User Guide*, while guidance for populating specific CISS POA&M and FA fields is provided in this document. The CISS application is available for download on the CMS Information Security Library Web page: http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp. (For CMS internal systems, submit a trouble ticket to have the CISS installed on your government laptop or PC.) The *CISS User Guide* is included in the CISS as a help file but it is also available as a download on this same Web site.

5 CISS FISMA ASSESSMENT (FA) PROCEDURES

The annual FA is an audit type; therefore, it is included as a module in the CISS audit security element node. The FA audit functions in conjunction with other audits and POA&M reporting and tracking processes within the CISS. For the annual FA, entities enter text responses to a subset of the full CMS Minimum Security Requirements (CMSRs) indicating the entity's status towards compliance with CMS minimum security requirements. In this manner, CMS entities are able to perform and document their required annual systems security FAs.

The CISS FA audit module allows CMS management and its entities to:

- Develop, maintain, and issue uniform, enterprise-wide systems security policy
- Perform annual FAs using standardized assessment methods
- Review CMSR controls in preparation for audits by specific federal and CMS organizations
- Develop, maintain, and evaluate a central repository for current and historical systems security program data
- Perform automated data entry of current systems security program data
- Perform automated reporting of current and historical systems security program data
- Perform concurrent data-entry or viewing by multiple qualified security representatives
- Track the status of open issues

The CISS also assists entities by validating and preparing the FA data file for submission to CMS as part of their annual certification package (refer to *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedures*). The CISS FA module provides entities with a powerful reporting tool that also generates formatted FA worksheet forms, copies of the CMS CMSRs, and standardized submission reports.

All CMS entities shall complete their annual CISS FA and submit a separate copy for each entity type (refer to Section 5.1.1 for entity types) to their respective CMS Business Owners. All CISS FA submissions shall be made to the respective Business Owner for all entity types by close of business on the first business day of May each calendar year unless specified otherwise in writing by the CMS Chief Information Security Officer (CISO). A copy of the completed annual FA shall be included in the entity’s System Security Profile.

CMS internal system/application entities should contact their respective Business Owners to determine how the annual FA should be submitted (i.e., email attachment, CD-ROM). For external system/application entities (i.e., business partners/contractors), the annual FA shall be submitted on CD-ROM to the CMS Central Office (CO) and the Consortium Contractor Management Officer (CCMO) for Title XVIII contracts, and the CMS Project Officer (PO) for Federal Acquisition Regulation (FAR) contracts. This information may not be submitted via email. Instead, Registered Mail™ or its equivalent shall be used. If technical assistance is needed, contact the CMS/Northrop Grumman help desk at (703) 272-5725.

5.1 COMPLETING THE FISMA ASSESSMENT (FA)

A critical factor for maintaining on-going compliance with federal requirements is for CMS Business Owners in coordination with developers, maintainers, and system operators, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person hours (if internal personnel are to be engaged in this activity). Entities are required to schedule and perform the test; and oversee the development and completion of corrective action plans (CAP) for vulnerabilities noted during the testing.

The annual FA requirement has been interpreted by the OMB as being within 365 calendar days of the previous FA. For CMS information systems, all controls applicable to a system or application shall be tested over a 3-year period. This means that a subset consisting of no less than 1/3 of the available security controls shall be tested each year so that all available controls are tested during a 3-year period. This annual subset is inclusive of the required annual test requirement of the system or application Contingency Plan.

While CMS does not mandate which specific subset of controls shall be tested each year or require a specific number (other than at least 1/3) of controls be tested each year, CMS does require that all controls be tested within a 3-year cycle. Business Owners, in coordination with the developer/maintainers of CMS applications and systems, are responsible for meeting this requirement.

5.1.1 INDEPENDENCE OF THE ASSESSMENT

To fulfill the annual FA validation obligation, the FA shall be conducted by an independent agent or team. This can be any internal or external agent or team that is capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

All management-directed and independent testing conducted with 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., FA) testing. Management directed and independent testing includes:

- Certification and accreditation (C&A) independent security test and evaluation (ST&E) testing
- OMB Circular A-123 IT Electronic Data Processing (EDP) assessments
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) Section 912 evaluations
- MMA Testing
- Statement on Auditing Standard (SAS) 70 reviews
- Certification Package for Internal Controls (CPIC) audits
- Government Accounting Office (GAO) reviews
- FA testing
- Chief Financial Officer (CFO) audit of CMS financial statements
- Testing results from local test teams (i.e., organizationally separated from the Medicare operations team) organized for purposes of meeting the FA requirement

Annual security controls testing, including FA testing, should be used to satisfy the requirements for the ST&E which is an integral component of the CMS C&A Program. In order to be considered as part of a system's or application's ST&E, the annual security control testing shall meet the standards for independence.

5.1.1 ENTITY TYPE SELECTION

The FA control selection is dependent on several factors determined through a data parameter "interview" process. The primary selection factor in this process is the entity type, and CMS minimum security control requirements:

- ABMAC: A/B Medicare Administrative Contractor
- COB: Coordination of Benefits
- CWF: Common Working File (Host)

- DC: Data Center
- DMEMAC: Durable Medical Equipment Medicare Administrative Contractor
- EDC: Enterprise Data Center
- PartA: Part A Fiscal Intermediary
- PartB: Part B Carrier
- PSC: Program Safeguard Contractor
- QIC: Quality Integrity Contractor
- RAC: Recovery Audit Contractor
- SS: Standard System (Maintainer)
- ZPIC: Zone Program Integrity Contractor
- Other: This entity type shall be selected when the entity is not one of the above predefined entity/contract types (e.g., CMS internal systems/applications) or when directed by the CMS Business Owner

5.1.1 SECURITY LEVEL AND DATA TYPE SELECTION

Once an entity type has been selected, the next step is to select the information system security level, information data type(s), and security control source document(s). In some cases, such as with most CMS business partner contract types, these selections are already made by the CISS based on CMS specified minimum control requirements and cannot be changed. In other instances, some selections are based on CMS-specified minimum control requirements but other selections can be selected by the entity, as necessary. When an “Other” entity type is selected, the entity must make all the selections based on input from the Business Owner.

When the entity type information data parameters are not pre-selected by the CISS, the information data security level (i.e., Low, Moderate, or High) shall be specified by the Business Owner. The CISS selectable information data type(s) processed, transmitted, and/or stored on the entity’s system are: electronic Personal Health Information (PHI or ePHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA), Federal Tax Information (FTI) as defined in Internal Revenue Service (IRS) Publication 1075 (*Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*), and Personally Identifiable Information (PII) as defined by the Privacy Act. The selectable control source documents are: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as amended, (*Recommended Security Controls for Federal Information Systems*)/800-53A, as amended, (*Guide for Assessing the Security Controls in Federal Information Systems*), *CMS Policy for the Information Security Program* (PISP)/*CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements* (CMSR), and *Federal Information System Controls Audit Manual* (FISCAM).

Certain data type parameters are “not selectable” when a “Low” security level is specified. For example, the minimum security level for HIPAA, IRS, and PII data is “Moderate,” so these data types cannot be selected with a “Low” security level. If any of these data types are processed, transmitted, and/or stored on an entity’s information system, the minimum security level must be specified as “Moderate”—then those data types may be included.

5.1.2 SECURITY CONTROL SELECTION

After the information system security level, information data type(s), and security control source document(s) are selected, the CISS uses these selections to determine which baseline controls apply to the entity type. It then presents only those applicable baseline controls for FA selection. Enhancement controls are not displayed on the selection form because they are included automatically with any baseline control selected.

Since the controls displayed and available for the FA selection are dependent on the entity type, information system security level, information data type(s), and security control source document(s) selections, it is paramount that Business Owners identify the appropriate security level categorization for their information and information system, and convey this information to the FA auditors.

5.2 SECURITY CONTROL ASSESSMENT

Security evaluations and/or testing (e.g., the FA) are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits. Rather, they are the last line of defense in the process of identifying the strengths and weaknesses of the entity’s information system that supports critical federal applications and missions in a global environment of sophisticated threats. The findings produced by security assessors during the FA are used primarily to determine the overall effectiveness of the security controls in an information system, and to provide credible and meaningful inputs to the entity’s security accreditation process. A well-executed security assessment helps to determine the validity of the security controls identified in the information System Security Plan (SSP) and to facilitate a cost-effective approach to correcting any deficiencies in the system in an orderly and disciplined manner consistent with the entity’s mission requirements.

Annual FAs using the assessment procedures (i.e., assessment objectives, and assessment methods and objects) provided with each CMSR are not intended to make judgments on the necessity or sufficiency of the set of security controls documented in the SSP. Rather the assessment procedures are applied to determine if the security controls employed (and required under CMS Policy) within the information system are, in fact, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Assessors, in the course of executing the CMSR assessment procedures, might discover potential errors or oversights in the security plan and determine how those potential errors or oversights may affect the confidentiality, integrity, and/or availability (CIA) of the information system in the event of a compromise or breach of the system. Such discoveries and determinations; however, are a by-product of the assessment and not the purpose of the assessment. Therefore, while assessors are expected to notify appropriate organizational officials about any potential problems with the SSP, assessors are not empowered to second-guess or question the decisions of Business Owners and authorizing officials concerning the impact level of the information system or the security control selection and supplemental activities, which include the tailoring and supplementation of the CMSR baseline controls.

The assessor results for each control requirement are aggregated and documented in the CISS "Audits" FA module (refer to *CISS User Guide* Section 4). They serve as a primary information source for the POA&M. The assessor does not prepare the POA&M, but may provide recommendations for its content. The Business Owner may have an opportunity to address some or all of the weaknesses or deficiencies in the security controls identified during the assessment before those weaknesses or deficiencies become part of the POA&M. However, senior leadership involvement in the mitigation process may be necessary in order to ensure that the entity's resources are effectively allocated in some priority order—first providing resources to the information systems that are supporting the most critical and sensitive CMS missions. Each identified finding and corresponding weakness shall be addressed with a CAP in the CISS before submitting the FA results to CMS management.

Ultimately, the assessment results and any subsequent mitigation actions initiated by the Business Owner in collaboration with designated organizational officials trigger updates to the Information Security (IS) Risk Assessment (RA) and the SSP. As a result, the key documents (i.e., SSP with updated IS RA, security assessment report, and POA&M) used by the authorizing official to determine the security status of the information system are updated to reflect the results of the security assessment.

5.3 SECURITY CONTROL COMPLIANCE

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the information necessary to make the determination associated with each assessment objective. Each determination statement in a procedural step contained within an assessment procedure executed by an assessor produces one the following results: "Met" or "Not Met." These assessment results are described in Table 1.

Table 1 Assessment Results

Level	Description
Met	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.
Not Met	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the entity.

A result of "Not Met" may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement. The assessor results (i.e., the determinations made) shall be an objective reporting of what was found concerning the security control assessed. For each assessment result other than "Met," assessors shall indicate which parts of the security control are affected by the finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state.

Any potential for compromises to CIA due to a “Not Met” finding shall also be noted by the assessor.

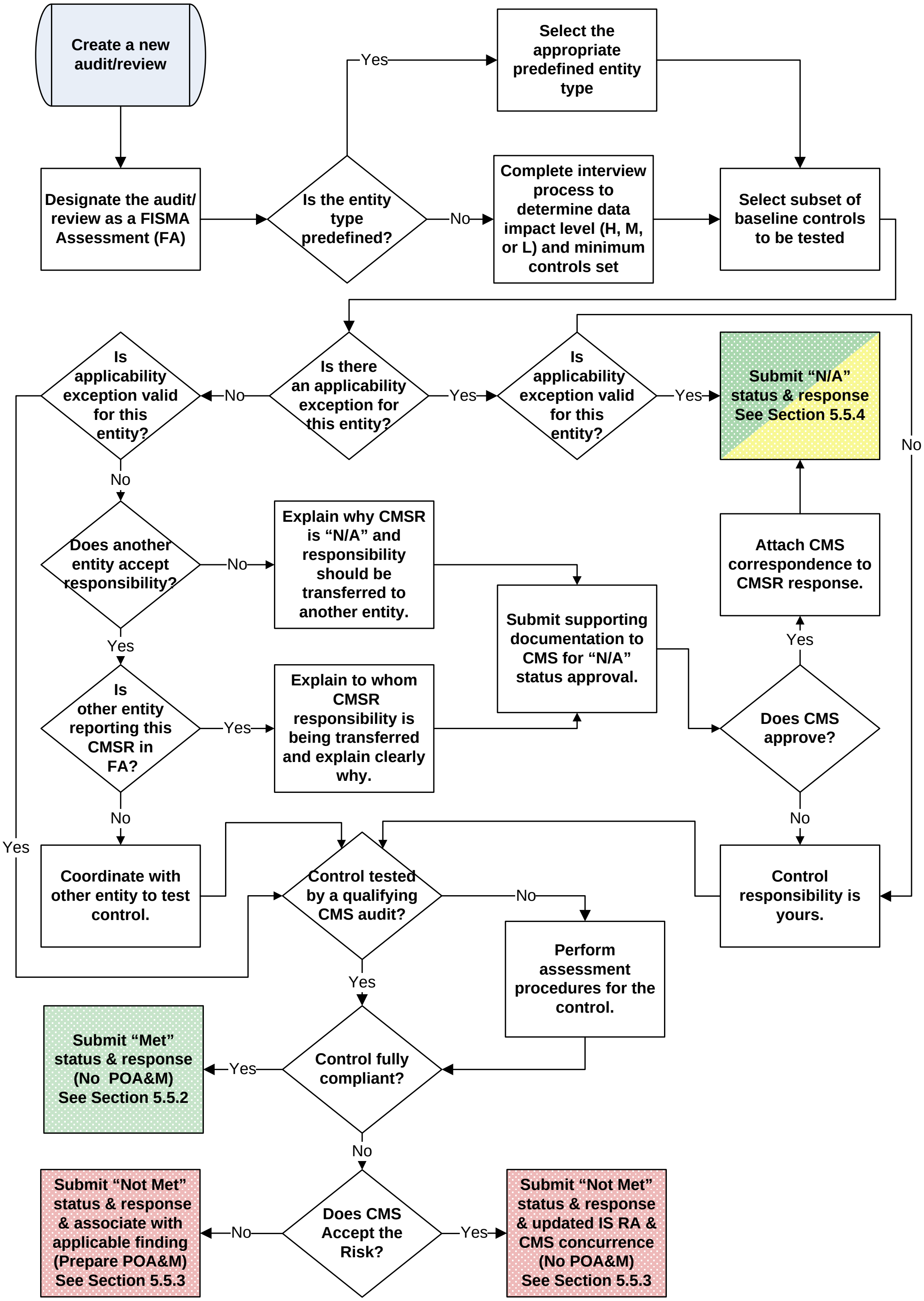
5.4 COMPLIANCE RESULT DETERMINATION

In the CISS FA module, testing individual CMSR compliance will result in one of two FISMA compliance results (or statuses): “Met” or “Not Met.” Other than the “N/A” result (which indicates that a control requirement does not apply as explained in Section 5.5.2), “Met” and “Not Met” are the only CMSR compliance results available in the CISS to report an FA status. To determine compliance, the CMSR assessment procedures shall be applied to determine if the security controls as employed within the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the applicable security requirement.

CMSRs include baseline and enhancement controls. Baseline controls are the minimum security controls recommended for an information system based on the system’s security categorization. Enhancement controls provide additional, but related, functionality to a baseline control; and increase the strength of the baseline control. Baseline controls may also include implementation standards which provide a tailored CMS definition or event with a value, such as “90 days”, which must be implemented and audited. Each baseline and enhancement control is assessed separately and its compliance status is recorded separately.

The decision tree in Figure 1 was developed to assist entities establish their CMSR compliance result (or status) for each baseline and enhancement control. Start with “Create a new audit/review” to establish the CMSR compliance status.

Figure 1 Response Status Decision Tree


Create a new audit/review
Designate the audit/ review as a FISMA Assessment (FA)
Is the entity type predefined?
Yes
Select the appropriate predefined entity type
No
Complete interview process to determine data impact level (H, M, or L) and minimum controls set
Select subset of baseline controls to be tested
Is there an applicability exception for this entity?
No
Is applicability exception valid for this entity?
Yes
Is applicability exception valid for this entity?
Yes
Submit "N/A" status & response See Section 5.5.4
No
No
Does another entity accept responsibility?
No
Explain why CMSR is "N/A" and responsibility should be transferred to another entity.
Submit supporting documentation to CMS for "N/A" status approval.
Attach CMS correspondence to CMSR response.
Yes
Does CMS approve?
Yes
Is other entity reporting this CMSR in FA?
Yes
Explain to whom CMSR responsibility is being transferred and explain clearly why.
No
Yes
Coordinate with other entity to test control.
Control tested by a qualifying CMS audit?
No
Perform assessment procedures for the control.
No
Control responsibility is yours.
Yes
Submit "Met" status & response (No POA&M) See Section 5.5.2
Yes
Control fully compliant?
No
Submit "Not Met" status & response & associate with applicable finding (Prepare POA&M) See Section 5.5.3
No
Does CMS Accept the Risk?
Yes
Submit "Not Met" status & response & updated IS RA & CMS concurrence (No POA&M) See Section 5.5.3

5.5 CMSR RESULT/RESPONSE REQUIREMENTS

All entities are required to enter a current compliance result (i.e., “Met,” “Not Met,” or “N/A”) and a detailed response comment/explanation in the CISS “Control Response” form for each CMSR evaluated. The annual FA is one of the central security documents in an entity’s System Security Profile and the FA shall reflect sufficient detail to convey to CMS Business Owners and management the current status of the entity’s security program.

5.5.1 ALL CMSR RESPONSES

The following information and guidance shall be considered when evaluating all CMSRs and completing CISS CMSR responses:

1) Every CMSR response requires a compliance “Result” (i.e., “Met,” “Not Met,” or “N/A”) to be selected, accompanied by a detailed explanation in the “Response” field that provides a complete description of why and/or how each CMSR control element is or is not met.

2) Every CMSR “Response” field should include a reference to the applicable FA working papers section, paragraph, or page where the applicable assessment procedure was performed and documented. (A single copy of the FA working papers shall be attached electronically to the CISS FA audit record. This is performed on the FA audit screen.)

3) Every CMSR response requires that a principle point-of-contact (POC) be designated. The CISS provides a specific field for this information and this field requires that at least one POC value be entered. Other involved POCs may also be assigned as non-primary designees. However, one and only one primary POC can be assigned to each CMSR response.

4) Entities should be aware that even if data processing duties are subcontracted to another CMS entity (such as a data center) or to a third-party subcontractor (such as a business services company), responsibility for the implementation and evaluation of security controls ultimately resides with the primary CMS contract holder or Business Owner. Entities shall coordinate the establishment of boundaries for specific issues. While this does not necessarily require a sharing of FA data, it does require that entities communicate and coordinate among themselves such that interfaces of responsibilities for all CMSRs are addressed by all responsible entities without any gaps in coverage. The CMS Business Owner is responsible for ensuring that all entities are properly addressing all faucets of each control.

5) Where a merging of responsibilities occurs among entities (such as the interface between data centers, claims processors, and standard systems), a detailed description of these interfaces and the division of responsibilities shall be provided in the response field. The description shall include local responsibilities as well as those perceived to be responsibilities of some other entity. However, this perception of responsibility shall not reference third-parties who do not perform and submit a corresponding FA to CMS.

6) Each CMSR in the CISS includes an “Applicability Exception(s)” field, which identifies the CMS contract/entity types (i.e., ABMAC, Part A, Part B, CWF, etc.) where each CMSR may

not apply. However, the purpose of the "Applicability Exception(s)" field is not to summarily exclude CMSRs from a particular contract/entity type. The "Applicability Exception(s)" field is designed to be used as a guide. CMS recognizes that system configurations vary widely throughout the CMS community. Therefore, each entity shall evaluate and report on each CMSR's applicability as it relates to its own system.

Note: Each "N/A" response status must still include a description of any controls that meets the intent of the requirement or a thorough explanation of why the control requirement is not applicable. If the control requirement is fulfilled by another entity, a summary explanation of what the other entity does is still required to ensure that the intent of the control is being met for the given process.

7) Entities should also be aware of the terms included in the CMS Information Security Terms & Definitions (http://www.cms.hhs.gov/informationsecurity/downloads/termsdefinitions.pdf) and address the CMSR security controls as they apply to their local environment.

   For example, the term "data center" refers to a "computer facility" which is defined as "a site or location with computer hardware where information processing is performed" (e.g., claims entry and processing facility). This term is not limited to EDCs or entity data centers. A "system" may include mainframe systems, desktop computers, workstations and servers, networks, and any platform regardless of its operating system. "System software" includes the operating system and utility programs (e.g., workstation, server, and network software and utilities) and is distinguished from application software. "Application software" includes CMS standard systems as well as any computer program (i.e., application) that manipulates data or performs a specific function (e.g., front-end and back-end applications).

8) If organizational policy conflicts with a CMSR, a detailed explanation shall be provided as to why the entity policy cannot be modified to apply to CMS data. Any conflicts with organizational policy (in which the final disposition of the CMSR response would not ultimately result in full compliance with CMS requirements) shall be addressed for resolution, by written correspondence with the CMS CO, prior to indicating such a non-compliance status for any CMSR.

5.5.1 "MET" RESPONSE RESULT

A CMSR compliance status of "Met" implies that the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result. The CISS "Control Response" form "Response" field shall, at a minimum, contain a detailed explanation of how the objectives of the CMSR are met, and how compliance can be verified, in a format that clearly answers each of the following questions:

- What can be used to verify full compliance with the CMSR objectives?

  While not required to be attached as supporting documentation in the FA submission, documentation in the form of policies, procedures, manuals, training records, and logs should be available to verify compliance. A description of these documents shall be included in the CMSR "Response" field. The control shall be tested using the CMSR assessment procedures (i.e., assessment objectives, and assessment methods and objects) to verify compliance. All documentation specified in the CMSR shall be verified for a response to be considered complete.

- Where can the applicable evaluation documentation be found?

  Verification of the performance of the applicable assessment procedures for each CMSR is a fundamental part of the FA process. Methods of verification in accordance with the applicable CMSR assessment procedures should be accessible to assessors. Ensure that a cross reference to section/page/paragraph in the working papers of the applicable audit/review documentation is clearly described. The applicable referenced working papers shall be included (electronically) to the FA audit record in the CISS. If another audit/review is cited as the source of testing, applicable working papers for the referenced audit/review shall also be included (electronically) with the FA submission.

- How exactly are the CMSR assessment objectives being met?

  - Do not include planned controls or controls that are not fully implemented as the basis for compliance. If any security control components are not fully implemented, the response result shall be changed to "Not Met" and a suitable finding/weakness/action plan combination shall be identified.

  - In some cases, alternative controls may be implemented to achieve the intent of the CMSR. Ensure that information about the implementation of alternative controls to meet the specifics of the CMSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

5.5.1 "NOT MET" RESPONSE RESULT

A CMSR compliance status of "Not Met" implies that the assessment information obtained during the evaluation indicates potential anomalies in the operation or implementation of the control that will need to be addressed by the entity. A result of "Not Met" may also indicate that for reasons specified in the assessment report (and entered in the CISS "Control Response" form "Response" field), the assessor was unable to obtain sufficient evidence to make the particular determination called for in the assessment objectives.

For each assessment result of "Not Met," assessors shall indicate which parts of the security control are affected by the assessment finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state, and this information shall be included in the applicable CMSR "Response" field.

The outcome of a "Not Met" CMSR response status results in one of the following:

- **Finding**: The result of each CMSR baseline and enhancement control shall be fully compliant (i.e., "Met"). For any response status that is not fully compliant, an appropriate finding and associated weakness/action plan combination shall accompany the CMSR response.

- **Risk-Based Decision**: In extremely rare instances, full compliance of a CMSR may present unacceptable fiscal or configuration barriers. In such cases, CMS may agree that the risk is acceptable for the present and no finding/weakness/action plan combination is required or desired. In such cases, prior written CMS concurrence is required and a full assessment of all of the implications for not being in full compliance of the minimum security requirements for the applicable CMSR is fully documented in the associated system Information Security (IS) Risk Assessment (RA). Both the updated IS RA and full documentation of CMS concurrence shall be electronically attached to the CMSR record in the CISS.

5.5.2 "N/A" (NOT APPLICABLE) RESPONSE RESULT

A CMSR response status result of "N/A" implies that the CMSR may not be applicable to the entity. CMS expects most, if not all, CMSRs to apply to all CMS contracts and entities (to some level), and expects all CMSRs to be evaluated as to their applicability. Very few CMSRs are expected to be completely non-applicable. The CISS "Control Response" form "Response" field shall contain a detailed explanation of the circumstances that render a CMSR non-applicable regardless of whether the contract/entity type is listed as "Optional" in the CISS "Applicability Exception(s)" field, and how this information can be verified, in a format that clearly answers each of the following questions:

- Why is this CMSR not applicable?

  A complete and detailed description shall be provided to describe the circumstances that render the result "N/A" to a particular entity. Simply referring to the "Applicability Exception(s)" field is not sufficient justification for a "N/A" result. A full understanding of the reasons for non-applicability shall be demonstrated and explained in the "Response" field. This is necessary because the "Applicability Exception(s)" field is not meant to be authoritative. CMS anticipates cases where a CMSR will apply to one or more entities even when the CISS "Applicability Exception(s)" field lists the CMSR as "Optional."

- How did you verify the "N/A" status?

  - **"Applicability Exception(s)" field indicates CMSR is "Optional"**: CMS approval is not required for an "N/A" result that is corroborated by the CMSR "Applicability Exception(s)" field (i.e., applicability is listed as "Optional"). However, a CMSR explanation is required amplifying why the entity agrees that the CMSR is not applicable.

  - **"Applicability Exception(s)" field indicates CMSR is applicable**: CMS approval is required for an "N/A" result that is not corroborated by the CMSR "Applicability Exception(s)" field (i.e., applicability is not listed as "Optional"). In this case, CMS approval shall be obtained and documented, and such approval (e.g., email or letter) shall be electronically attached to the CISS CMSR record.

- What documentation is provided with the "N/A" status?

  - No documentation is required when an "N/A" result is corroborated by the CMSR "Applicability Exception(s)" field (i.e., applicability is listed as "Optional").

  - CMS approval documentation (e.g., email or letter) is required when an "N/A" result is not corroborated by the CMSR "Applicability Exception(s)" field (i.e., applicability is not listed as "Optional"). CMS approval must be renewed each year for each CMSR "N/A" result that is not corroborated by the "Applicability Exception(s)" field unless CMS specifically stated otherwise in a prior approval citation. Prior year approvals may be cited in the written approval request that is submitted to the CMS Business Owner for a current year request, but prior year approvals shall not be used to fulfill the documentation requirement for a current year CMSR “N/A” result.

- In addition to the previous stated requirements, the following information shall be included in the “Response” field of each CMS-approved “N/A” status result:
  - Date CMS approved the request
  - CMS office that approved the request

6 CISS FINDINGS AND WEAKNESSES

A finding is any deficiency identified and reported during any internal or external audit or review.

- Finding example: “System administrator password easily cracked.”

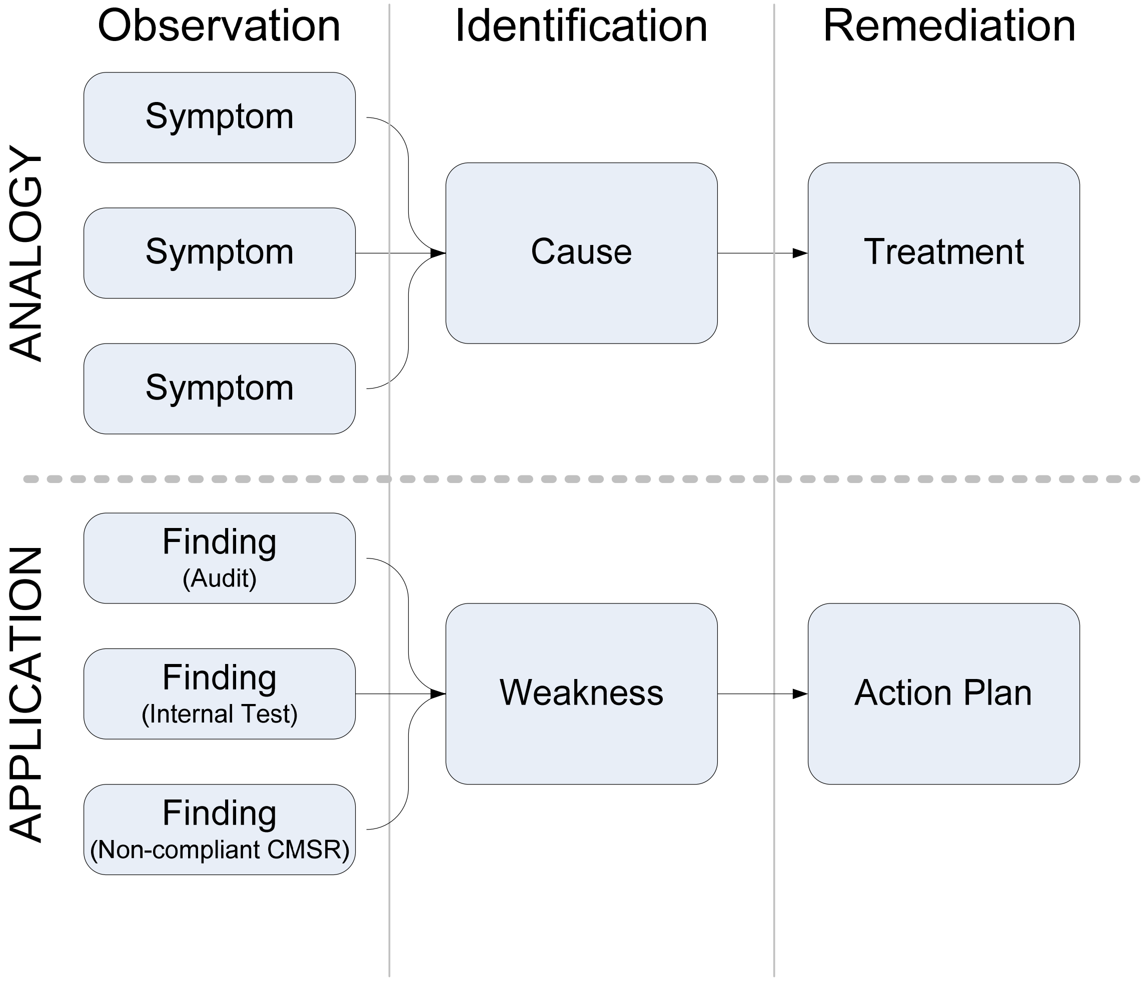
A weakness, in this context, is the underlying cause for, or source of, the finding.

- Weakness example: “System does not adhere to password policy.”

Security-related audit/review findings, which include FA non-compliant CMSR findings, form the basis for security-related weaknesses. Weaknesses in turn form the basis for action plans. Action plans address the correction actions necessary to remediate weaknesses and any findings attributed to the weakness (refer to Section 7 for more information on action plans and POA&Ms). Although all of these security elements (i.e., audit/review, finding, weakness, and action plan) are individual records in the CISS, they can be linked to, or associated with, each other.

An FA finding can be associated with one or more non-compliant CMSRs, but only if the security controls or assessment findings are related. A weakness shall be identified for each finding. However, a single weakness may address several findings. Consider the following simplified illustration:

Figure 2 Analogy for Finding-Weakness-Action Plan Relationship



Weaknesses that need to be recorded and tracked can be identified either reactively or proactively. Reactive weakness determination indicates that outside auditors/reviewers identified findings leading to the weakness determination. Proactive weakness determination occurs when conducting regular program and system reviews using internal reviews, periodic scanning, or controls monitoring. Sources of security-related findings and weaknesses include, but are not limited to:

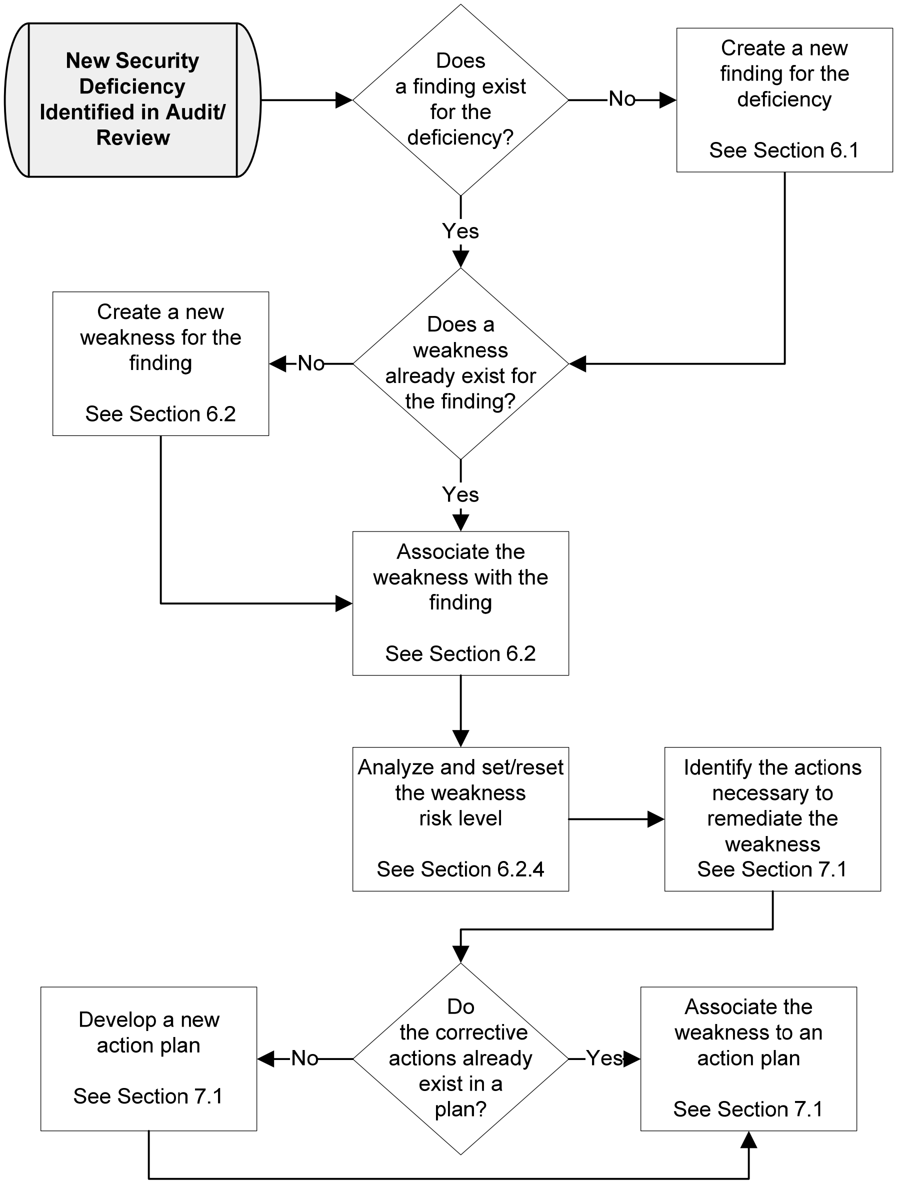
- Chief Financial Officer (CFO)/Electronic Data Processing (EDP) Audits related to annual CFO Financial Statement Audits (which may include Network Vulnerability Assessment/Security Testing [NVA/ST])
- Statement on Auditing Standards (SAS) No. 70 Audits
- Submission of a Certification Package for Internal Controls (CPIC)
- Department of Health and Human Services (DHHS), Office of Inspector General (OIG) Information Technology (IT) Controls Assessment
- General Accounting Office (GAO) Financial Reviews

- Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003 Section 912 Evaluation or Testing
- Data Center Security Test and Evaluation (ST&E)
- Penetration/External Vulnerability Assessment (EVA) test
- FISMA Assessment (FA)
- Information Security Risk Assessments
- Internal or self-directed reviews, audits, or tests
- Continuous monitoring activities

The previous listing is not exhaustive—there are many avenues for discovering weaknesses. In the CISS, all findings and weaknesses are considered to have resulted from some type of audit or review (either formal or informal.)

The flow in Figure 3 was developed to assist entities to establish the linkage among findings, weaknesses, and action plans. Start with "New Security Deficiency Identified in Audit/Review" to establish the linkage.

Figure 3 Weakness Decision Tree


New Security Deficiency Identified in Audit/ Review
Does a finding exist for the deficiency?
No
Create a new finding for the deficiency
See Section 6.1
Yes
Does a weakness already exist for the finding?
No
Create a new weakness for the finding
See Section 6.2
Yes
Associate the weakness with the finding
See Section 6.2
Analyze and set/reset the weakness risk level
See Section 6.2.4
Identify the actions necessary to remediate the weakness
See Section 7.1
Do the corrective actions already exist in a plan?
No
Develop a new action plan
See Section 7.1
Yes
Associate the weakness to an action plan
See Section 7.1

6.1 FINDINGS

All security-related findings identified or reported by internal or external audits/reviews shall be entered into the CISS and associated with (i.e., linked to) a weakness.

The following subsections provide guidance for populating the CISS “Findings” form. Refer to *CISS User Guide* Section 5 for specific instructions on completing the “Findings” form.

6.1.1 FINDING IDENTIFIER

The CISS “Findings” form identifier information is normally the same as provided in the audit/review report. If an internal finding is identified, the finding is recorded by a unique identifier consisting of the following information:

- **Entity**: The first 3–5 characters identify the name of the entity. These entity identifiers are listed in the *Medicare Financial Manual* (CMS Pub 100-6), Chapter 7, Internal Control Requirements, Section 40.3, CMS Finding Numbers, or (if not included in CMS Pub 100-6), are provided by the CMS Business Owner through coordination with the CISO or their designate. Since the entity identifier is stored in the CISS, this field is populated automatically.

  Note: This unique entity identifier is not reported to agencies outside of CMS nor is it included in CMS' annual or quarterly POA&M submission to OMB. Findings reported outside CMS cannot be traced to a CMS entity or contractor.

- **Year**: The next 4 digits denote the **fiscal** year (FY) in which the finding was identified and first reported. The year is normally the same as assigned in the audit/review report.
- **Code**: The next 1–2 characters identify the type of audit/review. This code is predefined and is selectable from a CISS drop-down menu.
- **Num**: The next 3 digits are a sequential finding number assigned to each individual finding (beginning with 001, 002, 003, etc.). The number is normally the same as assigned in the audit/review report or assigned as necessary for internal audit/review findings.

Note: If the finding number identified through an approved audit or review is not provided by the assessor in the above format, contact the CMS Business Owner for further guidance.

6.1.1 FINDING TITLE AND DESCRIPTION

The CISS “Findings” form “Title” field shall not include any entity-, location-, or system-specific information, or other sensitive or identifying information. This field is utilized, as written, for submission outside of CMS and could be used to specifically identify the entity reporting the finding, or the location, facility, system, or application to which the finding refers, which could expose the weakness to the public, thus making it easier to exploit. Some appropriate finding title examples include: “inadequate password controls,” “insufficient or inconsistent data integrity controls,” “inadequate firewall configuration reviews,” “background investigations not performed prior to system access,” “insufficient physical access controls,” etc.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information, such as: “Telnet port open, allowing access by outside users.” The title shall be unique enough so the finding is more readily identifiable by name than by number. The finding title reported in the audit/review report shall generally be used, unless that title is too long or it contains sensitive descriptive information.

The information included in the CISS “Findings” form “Description” field is not reported beyond CMS management, so there is no restriction on its content. The description shall normally be the descriptive information reported in the applicable audit/review report. If the finding is the result of an internal audit/review, the description shall include the finding information required by the GAO Government Auditing Standards, GAO-07-731G (http://www.gao.gov/new.items/d07731g.pdf), commonly referred to as the "Yellow Book."

6.1.1 FINDING STATUS

All security-related findings shall include a status that indicates the stage or state of the finding corrective action(s). Since a weakness may be associated with multiple findings, one or more findings associated with a weakness can be closed while the weakness remains open. The four CISS "Findings" form "Status" field drop-down selections are:

- **Ongoing**: The finding remains open and any action to correct it is ongoing. However, if the CISS "Action Plan" form "Initial Target" date "Completion Dates" field has passed and action is still ongoing to correct the weakness, the status shall be reported as "Delayed."
- **Closed Pending**:
  - If the finding was discovered by an internal audit/review, the entity may proceed directly to a "Closed" status.
  - If the finding was reported by a CMS-initiated audit/review, the entity should use this status when it considers the finding closed. However, CMS requires that this type of closure to be validated before CMS considers the finding status to be closed. The entity shall continue to report the finding status as "Closed Pending" until the closure is validated and CMS provides documentation to confirm the "Closed" status. The CISS requires that appropriate documentation be attached to the finding record to confirm the closure. The documentation shall address all aspects of the stated finding and be sufficient for CMS validation of closure.
- **Closed**: If a finding has been officially closed by the CMS Business Owner and submitted supporting documentation as closure proof to the entity, the finding status shall be reported as "Closed." The CISS requires that appropriate missing or updated documentation not previously sent be attached to the finding record to confirm the "Closed" status. This documentation shall include any CMS closure letters.
- **Delayed**: The status is "Delayed" when action is ongoing to correct the finding but the CISS "Action Plan" form "Initial Target" date "Completion Dates" field has passed. The finding shall continue to be reported as "Delayed" until the finding is corrected and reported as "Closed Pending" (CMS-initiated audits/reviews) or "Closed" (internal audits/reviews).

6.1.2 FINDING RISK LEVEL DETERMINATION

FISMA guidance requires that all weaknesses be prioritized to ensure that significant IT security weaknesses take precedence and are immediately mitigated. Since a finding indicates a weakness, a risk level shall also be assigned to each finding. The risk level determination process is summarized in Section 6.3, Determining Risk—the same determination process is used for findings and weaknesses.

After the CISS “Findings” form “Likelihood” and “Impact” field values have been selected, the overall finding “Risk” level field is calculated automatically based on these two values. Once a finding linked to a weakness that is reported to CMS in a POA&M, the “Likelihood” and “Impact” field values are locked and cannot be changed.

6.1.3 FINDING FMFIA AND CPIC SEVERITY

Findings, and their associated weaknesses, shall be disclosed as a “Material Weakness” or “Reportable Condition” if they have an impact on the entity’s internal financial control structure. Every finding identified as an internal financial control deficiency should be categorized as either a “Material Weakness” or “Reportable Condition” based on the following definitions:

- **Reportable Condition**: Exists when the internal controls are adequate in design and operation and reasonable assurance can be provided that the intent of the control objective is met, but deficiencies were found during the review that requires correction.
- **Material Weakness**: Exists when the entity fails to meet a control objective. This may be due to a significant deficiency in the design and/or operation of internal control policies and procedures. Because of these shortfalls in internal financial controls, the entity cannot provide reasonable assurance that the intent of the control objective is being met.

6.1.4 FINDING SECURITY CONTROL CATEGORY

All findings shall be assigned to a security control category. This security control category corresponds to the non-compliant CMSR baseline security control family (i.e., Access Controls for AC controls, Awareness and Training for AT controls, etc.). These security control families are selectable from a CISS drop-down list.

6.1.5 FINDING POINT(S) OF CONTACT

A primary POC shall be designated (or assigned) for each reported finding. While multiple POCs can be assigned to a finding, only one POC can be designated as the primary POC for each finding. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the finding. Non-primary POCs can include anyone who will assist the primary POC in resolving the finding.

6.2 WEAKNESSES

The term “weakness” refers to any program- or system-level IS vulnerability that poses a risk to the CIA of CMS’ information. Weaknesses represent the gaps between the current program or system status and the long-term program or system security objectives. All security-related weaknesses identified by internal or external audits/reviews shall be entered into the CISS and associated with (i.e., linked to) an action plan, and one or more findings.

Weakness remediation is the process whereby a security vulnerability is identified, corrective actions are initiated, and the weakness is properly mitigated. All security weaknesses that represent risk to the security of a program or system, and that require planned mitigation shall be identified in a CAP (i.e., action plan) and shall be captured and reported in a POA&M (refer to Section 7).

The following subsections provide guidance for populating the CISS "Weaknesses" form. Refer to *CISS User Guide* Section 6 for specific instructions on completing the "Weaknesses" form.

6.2.1 WEAKNESS IDENTIFIER

Each weakness shall be identified and recorded by a unique identifier. The CISS "Weaknesses" form identifier data consisting of the following information:

- **Entity**: The first 3–5 characters identify the name of the entity. These entity identifiers are listed in the *Medicare Financial Manual* (CMS Pub 100-6), Chapter 7, Internal Control Requirements, Section 40.3, CMS Finding Numbers, or (if not included in CMS Pub 100-6), are provided by the CMS Business Owner through coordination with the CISO or their designate. Since the entity identifier is stored in the CISS, this field is normally populated automatically.

  Note: This unique entity identifier is not reported to agencies outside of CMS nor is it included in CMS' annual or quarterly POA&M submissions to OMB. Weaknesses reported outside CMS cannot be traced to a CMS entity or contractor.

- **Quarter**: The next single character represents the FY quarter in which the weakness was first identified and entered into a POA&M, where:

  A = 1st Quarter

  B = 2nd Quarter

  C = 3rd Quarter

  D = 4th Quarter

- **Year**: The next 4 digits denote the FY in which the weakness was identified and first reported.

- **Number**: The next entry is an incremental number representing the sequence in which the weakness was entered into the entity's POA&M during the designated quarter and FY.

For example, a weakness identified as "CMS_B_2008_3" indicates this CMS Weakness was identified and first reported during the 2nd quarter of FY 2008, and it is the 3rd weakness identified during that time period.

6.2.1 WEAKNESS TITLE AND DESCRIPTION

The CISS "Weakness" form "Title" field shall not include any entity-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the entity reporting the weakness, or the location, facility, system, or application to which the weakness refers.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information. The title shall be unique enough so the weakness is more readily identifiable by name than by number.

The information included in the "Description" field is not reported beyond CMS management, so there is no restriction on its content. Detailed descriptions are neither necessary nor recommended; however, sufficient information is required to enable appropriate oversight and tracking, demonstrate awareness of the weakness, and articulate specific actions initiated to address the weakness.

6.2.1 WEAKNESS SECURITY CONTROL CATEGORY

All weaknesses shall be assigned to a security control category. This security control category corresponds to the non-compliant CMSR baseline security control family (i.e., Access Controls for AC controls, Awareness and Training for AT controls, etc.). These security control families are selectable from a CISS drop-down list.

6.2.2 WEAKNESS RISK LEVEL DETERMINATION

FISMA guidance requires that all weaknesses be prioritized to ensure that significant IT security weaknesses take precedence and are immediately mitigated. The risk level determination process is summarized in Section 6.3, Determining Risk—the same determination process is used for findings and weaknesses.

After the CISS "Weakness" form "Likelihood" and "Impact" field values have been selected, the overall weakness "Risk" level field is calculated automatically based on these two values. However, the "Likelihood" and "Impact" field values cannot be lower than the highest such values included in any findings linked to the weakness.

6.2.3 WEAKNESS FISMA SEVERITY

FISMA requires the reporting of any significant deficiency in a policy, procedure, or practice to be identified as a material weakness under the FMFIA, and if related to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (FFMIA). Depending on the risk and magnitude of harm that could result, weaknesses identified during the audit/review of security controls are reported as deficiencies in accordance with OMB Circular No. A-123, *Management Accountability and Control*, and FMFIA.

Although the CISS "Weakness" form "FISMA Severity" field includes the three available FISMA severity levels in a drop-down menu, only one level ("Weakness") is activated and available for selection by users. The other two severity levels, "Significant Deficiency" and "Reportable Condition," require that CMS make a risk-based decision before they can be assigned to a weakness. Should the CMS CISO make that determination, additional guidance or required actions will be provided to applicable Business Owners.

The three FISMA severity levels are:

- **Weakness**: This level refers to any and all other IT security weaknesses pertaining to the system. **Note:** This is the only severity level that can be selected at this time.
- **Reportable Condition**: This level exists when a security or management control weakness does not rise to a significant level of deficiency; yet, it is still important enough to be reported to internal management. A security weakness may be considered a "Reportable Condition" even though it is not deemed to be a "Significant Deficiency" by CMS management if it affects the efficiency and effectiveness of CMS operations. However, due to lower risk, corrective action may be scheduled over a longer period of time.
- **Significant Deficiency**: This level exists when a weakness in CMS' overall information systems security program or management control structure, or within one or more information systems, significantly restricts the capability of CMS to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the CMS head and outside agencies shall be notified and immediate or near-immediate corrective action shall be taken.

6.2.4 WEAKNESS TYPE

There are two types of security-related weakness that shall be identified. The CISS "Weakness" form includes the following two weakness "Type" selections:

- **Program Weakness**: This weakness type may impact multiple IT systems as a result of a deficiency in the overall IT security program.
- **System Weakness**: This type pertains to the management, operation, or technical controls of a specific IT system.

6.2.5 WEAKNESS STATUS

All security-related weaknesses require that a status be included that indicates the stage or state of the weakness corrective action. Since multiple findings may be associated with a single weakness, such weaknesses cannot be closed until all findings associated with it are closed. The four CISS "Weakness" form "Status" field drop-down selections are:

- **Ongoing**: The weakness remains open and any action to correct it is ongoing. However, if the CISS "Action Plan" form "Initial Target" date "Completion Dates" field has passed and action is still ongoing to correct the weakness, the status shall be reported as "Delayed."
- **Closed Pending**:
  - If the weakness resulted from a finding discovered by an internal audit/review, and the finding is closed, the entity may proceed directly to a "Closed" status.
  - If the weakness resulted from a finding discovered by a CMS-initiated audit/review, the entity should use this status when it considers the associated finding(s) closed. However, CMS requires that this type of finding closure to be validated before CMS considers the

finding status to be closed. The entity shall continue to report the weakness status as "Closed Pending" until the finding closure is validated.

- **Closed**: If all findings associated with a weakness have been closed officially by the CMS Business Owner, with supporting documentation submitted as proof to the entity, and the weakness itself is closed, the weakness status shall be reported as "Closed." Note that CMS concurrence is not required to report a weakness as "Closed" when all findings linked to the weakness are closed and the weakness itself is closed.
- **Delayed**: The status is "Delayed" when action is ongoing to correct the weakness but the CISS "Action Plan" form "Initial Target" date "Completion Dates" field has passed. The weakness shall continue to be reported as "Delayed" until any associated finding is corrected and reported as "Closed Pending" (CMS-initiated audits/reviews) or "Closed" (internal audits/reviews).

6.2.6 WEAKNESS POINT(S) OF CONTACT

A primary POC shall be designated (or assigned) for each reported weakness. While multiple POCs can be assigned to a weakness, only one POC can be designated as the primary POC for each weakness. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the weakness. Non-primary POCs can include anyone who will assist the primary POC in resolving the weakness.

6.3 DETERMINING RISK

The risk determination process explained in this section is taken from the CMS IS RA Procedures. The process described here assumes that specific threats and vulnerabilities have already been identified. Consult the CMS IS RA Procedures for specifics on identifying threats and vulnerabilities.

While both IS system and business risk measurements are combined in the CMS IS RA Procedures, the finding and weakness risk determinations included in this procedure pertain to IS risk determinations only. The goal of IS risk determination is to calculate the level of risk for each threat/vulnerability pair based on:

- The likelihood of a threat exploiting a vulnerability
- The severity of impact that the exploited vulnerability would have on the system, its data, and its business function in terms of loss of CIA

6.3.1 DETERMINING LIKELIHOOD OF OCCURRENCE

The risk likelihood level is determined by considering known threats as they may apply to known system vulnerabilities. The likelihood is an estimate of the frequency or the probably of such an event. The likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access, and existing controls; the presence, motivation, tenacity, strength, and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls.

Table 2 provides guidelines for determining the likelihood of occurrence level that the threat is realized and exploits the system's vulnerability.

Table 2 Likelihood of Occurrence Levels

Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur 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.

6.3.1 DETERMINING IMPACT SEVERITY

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

Table 3 provides guidelines for determining the system impact severity level.

Table 3 System Impact Severity Levels

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

6.3.1 DETERMINING THE OVERALL RISK LEVEL

The overall risk level can be expressed in terms of the likelihood of the threat exploiting the system vulnerability and the impact severity of that exploitation on the CIA of the system. This overall level of risk is depicted in the following equation:

- Risk Level = Likelihood of Occurrence X Impact Severity

After the risk likelihood of occurrence and impact severity are established, the overall level of risk is determined using the risk level matrix in Table 4. The level of risk equals the intersection of the likelihood of occurrence and impact severity values. The CISS determines the "Findings" and "Weakness" form "Risk" field value automatically based on the values selected in their respective "Likelihood" [of Occurrence] and "Impact" [Severity] field selections.

Table 4 Overall Risk Level Matrix

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

7 CISS ACTION PLANS AND POA&MS

FISMA requires that federal agencies (and their contractors) provide annual reporting of the state of security programs for all IT systems associated with the agency. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified security deficiencies (i.e., weaknesses) be addressed in a report (i.e., action plan) to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans. Action plans form the basis for the initial corrective action report as well as the periodic POA&M reporting requirement.

A POA&M is a management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The CMS IS Program POA&M process included in the CISS shall be used to facilitate the remediation of all IS program- and system-level weaknesses. This process provides a means for:

- Planning and monitoring corrective actions
- Defining roles and responsibilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources

- Informing decision makers

7.1 COMPLETING ACTION PLANS

Action plans form the basis for the periodic POA&M reporting requirement. Each weakness entered into the CISS shall correspond to an action plan for its resolution. Although the CISS does permit multiple weaknesses to be addressed by a single action plan, this approach is not recommended, because a weakness cannot be closed until its corresponding action plan has been completed.

Corrective action methods shall be analyzed for appropriateness in fully resolving any associated weakness; they should also be viewed for long-term implications. When completing an action plan, the cost for each option shall be estimated and analyzed to determine short- and long-term solution capabilities.

After the completion of all management-directed **external** audit/review, each entity must prepare an initial CAP for all audit/review findings within 30 days of the final audit/review report (unless otherwise directed by the CMS Business Owner). Entities shall use the following action plan and milestone procedures to complete the CAP. Then they shall refer to Section 7.2.1 for the initial CAP submission/approval procedures.

Note: Entities that utilize the CISS to prepare their corrective actions plan can produce a detailed CAP approval report directly from the CISS for submission to their Business Owner for approval (prior to POA&M data submission.)

7.1.1 ACTION PLAN TITLE AND DESCRIPTION

The CISS "Action Plan" form "Action Plan Title" field shall not include any entity-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the entity reporting the action plan, which location or facility has the weakness, or what system or application has the weakness. The title is used only to provide a descriptive name to the action plan so it can be distinguished from other action plans.

The information included in the "Description" field is not reported beyond CMS management, so there is no restriction on its content. Detailed descriptions are neither necessary nor recommended; however, sufficient information is required to enable appropriate oversight and tracking, and articulate the overall actions initiated to address the weakness.

7.1.1 DETERMINING COMPLETION DATES

The CISS "Action Plan" form "Completion Dates" fields ("Initial Target," "Current Projected," and "Actual") are populated automatically based on date fields included in the "Action Plan" form "Milestones" sub-form. The "Completion Dates" fields also update automatically until the action plan is reported in a POA&M submission.

Once an action plan has been submitted to the CMS Business Owner, the “Initial Target” field date is locked and cannot be changed. When completing individual milestones, completion dates in the “Milestones” sub-forms should be determined based on realistic timelines for resources to be obtained and associated steps to be completed. For example, although it may take 30 days to complete the required action plans for a specific weakness, it may not be possible to complete all weakness action plans during the same time period due to staffing resource limitations. Therefore, the “Milestone” sub-form “Initial Target” field date shall be based on the outcome of management review, prioritization decisions, and resource availability.

7.1.1 DETERMINING SECURITY COSTS

When determining the weakness remediation costs, entities shall consider the following criteria to determine security costs for a specific IT investment:

- The products, procedures, and personnel (entity employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. This includes the costs of:
    - Risk assessment
    - Security planning and policy
    - Certification and accreditation
    - Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
    - Authentication or cryptographic applications
    - Education, awareness, and training
    - System reviews/evaluations (including security control testing and evaluation)
    - Oversight or compliance inspections
    - Development and maintenance of entity reports to CMS and CAPs as they pertain to the specific investment
    - Contingency planning and testing
    - Physical and environmental controls for hardware and software
    - Auditing and monitoring
    - Computer security investigations and forensics
    - Reviews, inspections, audits, and other evaluations performed on entity facilities and operations
- Security costs shall include the products, procedures, and personnel (entity employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change

management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; system administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

- Many corporate entities operate networks that provide some or all of the necessary security controls for the associated applications, including CMS applications. In such cases, the entity shall nevertheless account for security costs for each application investment. To avoid "double-counting," entities shall appropriately allocate the costs of the network for each of the corporate and CMS applications for which security is provided.

In identifying security costs, entities may find it helpful to ask the following simple question: "If there were no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary; and what costs would be avoided?"

If entities encounter difficulties with the above criteria, they shall contact their CMS Business Owner prior to submission of their POA&M report.

When completing the CISS "Action Plan" form "Costs" fields, entities shall consider the following criteria when determining security costs and percentages:

- **Estimated Annual Maintenance**: This is the projected recurring cost to the CMS Business Owner (including depreciation, amortization, etc.) to maintain the remediation safeguard(s) for the following FY. Costs associated with continued funding shall be added to subsequent line one charges where applicable.
- **Percent Security**: This is the percentage of the total remediation safeguard costs that pertain or apply to security.
- **Percent Applied to CMS**: This is the percentage of the total remediation safeguard cost that the CMS Business Owner should fund for safeguards that will be shared between CMS (Medicare) systems and other systems where applicable.

7.1.2 DETERMINING FUNDING SOURCES

The "Action Plan" form "Funding Sources" fields allocate the total cost for implementing the remediation safeguard(s) during the first year of implementation. This shall include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Since this cost may be used for budgetary purposes, it shall be as accurate as feasible. It is advisable that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted when estimating this cost.

The CISS requires that funding resources be identified for every action plan. Action plans cannot be executed without the application of funding resources. Therefore, the CISS will not accept "zero-cost" action plans. Funding resources shall be entered in the following "Funding Sources" fields:

- **Current**: This is any existing resource already marked for security management of the system or program. This shall be the method most commonly used because security weaknesses need to be addressed in the near term.
- **Reallocated**: This is any other existing resource that must be reallocated to support the weakness mitigation.
- **New**: This is any additional funding that must be requested and allocated to complete the weakness mitigation. If new funding is required, the existing capital planning process shall be relied upon to request and receive the necessary funds.

  Note: Requesting new or additional funding from the CMS Business Owner to remediate a weakness shall only be used when no other source of funding can be identified. When funding is available, the CMS Business Owner must prioritize funding allocations based on weakness prioritization and risk levels. It is in the entity's best interest to use current resources or reallocate existing funds or personnel to remediate all weaknesses. All funding reallocations shall be approved by the CMS Business Owner.

7.1.3 ACTION PLAN MILESTONES

Milestones are the specific, action-oriented steps necessary to mitigate a weakness. The number of milestones articulated per weakness should directly correspond to the number of steps or corrective actions necessary to fully address and resolve the weakness. Each weakness must have at least one corresponding milestone with an anticipated completion date. The milestone completion date identifies the allotted time reserved to address the individual milestone and helps place milestones in a logical order. Milestones should effectively communicate the major steps that will be performed to mitigate a weakness.

Once milestones and completion dates are entered in the CISS "Milestones" sub-form within the "Action Plan" form and they are reported in a POA&M, changes cannot be made. If estimated milestone completion dates change, the new expected date must be recorded in milestone change (refer to Section 7.1.3.1).

7.1.3.1 MILESTONE TITLE AND DESCRIPTION

The CISS "Action Plan" form "Milestones" sub-form "Title" field shall not include any entity-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the entity reporting the milestone, which location or facility has the weakness, or what system or application has the weakness. The title is used only to provide a descriptive name to the milestone so it can be distinguished from other milestones in the same action plan.

The information included in the "Description" field is not reported beyond CMS management, so there is no restriction on its content. Detailed descriptions are neither necessary nor recommended; however, sufficient information is required to enable appropriate oversight and tracking, and articulate the overall actions addressed in the milestone.

7.1.3.1 MILESTONE COMPLETION DATES

Fundamentally, the action plan is simply a container for the milestones that address remediation of any corresponding weakness. The milestones are identified in the POA&M, and each one shall correspond to a specific corrective action. Ideally, there shall be at least one milestone per quarter so that action plan progress can be tracked in the POA&M submissions to CMS.

Including anticipated completion dates with each milestone enables progress toward weakness mitigation to be tracked. Each milestone within the POA&M shall include an anticipated date of completion (“Projected Date” field). Once milestones and completion dates are entered, changes can be made until the action plan is first submitted to the CMS Business Owner, at which time some milestone fields become locked and no longer can be changed.

The overall action plan projected completion date is derived automatically by the CISS based on the projected completion dates of all of the milestones. The “Initial Target” date field remains unchanged once the action plan has been submitted to the CMS Business Owner. However, the “Current Projected” date field will adjust automatically based on changes in milestone projected completion dates. (Note that an “Action Plan” form “Status” of “Delayed” is always based on the “Initial Target” date field.)

Milestones should effectively communicate the individual major steps within an action plan that shall be performed to mitigate a weakness. For example, appropriate milestones for an action plan associated with a weakness such as “Identification and authentication process needs to be more stringent” might read:

- Evaluate methods for strengthening identification and authentication
- Develop procedures to standardize accepted authentication process
- Acquire management approval/sign-off of new process and procedures
- Implement approved authentication process

7.1.3.1 MILESTONE UPDATES/CHANGES

Before the POA&M can be submitted to the CMS Business Owner each month, the progress of every open milestone previously reported in a POA&M must be updated to reflect its current state. In addition, every milestone must have at least one “Status Update” milestone that reflects its current “Status” and “Completion” state (refer to *CISS User Guide* Section 7.5.3). When entering a milestone update, entities should enter the current date (not a future date) in the “Status Update” sub-form “Date” field. However, in no case shall the status update “Date” field be a date that falls after the next POA&M submission date. The purpose of the status update form is to provide a milestone status update—not to make a milestone projected date change.

When a milestone is created and a date is entered in the “Milestone” sub-form “Projected Date” field, this date is displayed in the “Action Plan” form as the “Initial Target” and “Current Projected” date fields. Up until the time this milestone is submitted in a POA&M, this “Projected Date” field can be changed. However, once this milestone has been reported in a POA&M, this milestone date and “Initial Target” date is locked and cannot be changed. To revise the milestone completion projected date (i.e., to a projected earlier or later date), the new date must be entered in a “Projected Date” sub-form “Projected Date” field and a reason for the delay must be entered in the “Note” field (refer to *CISS User Guide* Section 7.5.2). This new date will then be shown in the “Current Projected” date field in the “Action Plan” form, but the “Initial Target” date will remain as originally projected.

Note: OMB reporting rules do not allow for the addition or subtraction of individual milestones within a CAP (after initial submission). if the substance of a milestone must be changed from the original plan, changes may be accounted for by updating the projected completion dates of the existing milestone(s), and entering the substance change (what changed in the milestone) in the “Note” field.

7.2 CAP/POA&M SUBMISSIONS

The CISS assists entities in collecting and reporting weaknesses, preparing action plans (including milestones), submitting the required initial CAP to the CMS Business Owner for approval, and submitting the POA&M in OMB format to the CMS Business Owner. The initial CAP approval report is described in *CISS User Guide* Section 4.10.3, Current Audit Approval Report, and the POA&M submission process is described in *CISS User Guide* Section 13, Submissions to CMS. The remainder of this section is devoted to the initial CAP submission/approval and POA&M submission procedures.

7.2.1 INITIAL CAP SUBMISSION

After the completion of all management-directed **external** audit/review, each entity must prepare an initial CAP for all audit/review findings within 30 days of the final audit/review report (unless otherwise directed by the CMS Business Owner). The corrective actions shall be established in a CISS action plan and its CAP report (refer to *CISS User Guide* Section 4.10.3) shall be submitted to the CMS Business Owner for approval **before** the planned corrective actions are reported in a POA&M. CAP approvals are not required for internal or self-directed reviews, audits, or tests.

The Business Owner may either approve the CAP(s) as submitted or he/she may request additional information to be included in the CAP(s). Responses to any Business Owner initial CAP comments shall be included in the respective action plan when it is reported in the next POA&M submission to CMS (refer to Section 7.2.1).

7.2.1 MONTHLY POA&M SUBMISSION

Unless otherwise directed by their CMS Business Owner, every CMS internal/external entity shall use the CISS tool to submit their monthly POA&M to their CMS Business Owner on the first business day of each month. These monthly POA&M submissions shall include updates on the progress towards completion of remediation efforts for all security-related weakness identified from all know known sources. A copy of the POA&M submission shall be included in the entity’s System Security Profile.

CMS internal system/application entities should contact their respective Business Owners to determine how the monthly POA&M updates should be submitted (i.e., email attachment, CD-

ROM). For external system/application entities (i.e., business partners/contractors), the monthly POA&M updates shall be submitted on CD-ROM to the CMS CO and the CCMO for Title XVIII contracts, and the CMS PO for FAR contracts. This information may not be submitted via email. Instead, Registered Mail™ or its equivalent shall be used. If technical assistance is needed, contact the CMS/Northrop Grumman help desk at (703) 272-5725.

(This Page Intentionally Blank)