

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850



***Framework for the Independent Assessment of
Security and Privacy Controls***

Final

March, 2016

Version 2.0

Record of Changes

Number	Date	Reference	A=Add, M=Modify, D=Delete	Description of Change	Change Request #
Version 1.0	07/2014		A	Initial draft release	
Version 1.2	10/2015		M	Address Privacy during the IA	
Version 1.9	01/2016		M	Incorporate Privacy requirements	
Version 2.0	03/2016		M	Incorporate comments and feedback	

Table of Contents

- 1. INTRODUCTION3
 - 1.1 Requirements Background.....3
 - 1.2 Purpose.....3
- 2. ASSESSMENT INDEPENDENCE4
 - 2.1 Options for Independent Assessors4
 - 2.2 Purpose of the Independent Security and Privacy Control Assessment4
- 3. ASSESSMENT PLANNING.....6
- 4. SECURITY AND PRIVACY CONTROL ASSESSMENT METHODOLOGY7
 - 4.1 Tests and Analyses Performed.....7
 - 4.1.1 Security Control Technical Testing8
 - 4.1.2 Network and Component Scanning8
 - 4.1.3 Configuration Assessment8
 - 4.1.4 Documentation Review.....9
 - 4.1.5 Personnel Interviews.....10
 - 4.1.6 Observations10
- 5. SECURITY AND PRIVACY ASSESSMENT REPORTING.....12
 - 5.1 Suggested Report Structure12
 - 5.1.1 SAR Content12
 - 5.1.2 Sample SAR Report Structure13
- APPENDIX A: SAMPLE SECURITY AND PRIVACY ASSESSMENT REPORT (SAR).....14

1. INTRODUCTION

The State-Based Administering Entities (AE) are custodians of sensitive information such as Personally Identifiable Information (PII) for millions of US citizens. As such, they have a unique responsibility for ensuring its ultimate protection. Through continuous monitoring and regular security and privacy control testing, the AE demonstrates that it meets this responsibility. This *Framework for Independent Assessment of Security and Privacy Controls* provides an overview of the independent security and privacy assessment requirements and the associated Centers for Medicare & Medicaid Services (CMS) reporting process for Administering Entities.

1.1 REQUIREMENTS BACKGROUND

The *CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)*¹ Security Assessment Control, CA-2, requires all security and privacy controls attributable to a system or application be assessed over a 3-year period. Additionally, the MARS-E Independent Assessor Control, CA-2(1), requires that this assessment be conducted by an “independent assessor,” sometimes referred to as a “third-party” assessor.

The Security and Privacy Control Assessment (SCA) assists CMS information security and privacy staff with understanding the current security and privacy posture of the Affordable Care Act (ACA) information system and its potential impact on the broader ACA program. The SCA also provides the means to identify potential opportunities for supplying targeted technical security and privacy assistance.

1.2 PURPOSE

The framework is designed to accomplish the following objectives:

- Define assessment independence and the independent assessor (Section 2)
- Provide assessment planning considerations (Section 3)
- Provide a basic security and privacy control assessment methodology (Section 4)
- Summarize security and privacy assessment reporting (Section 5)
- Provide a sample security and privacy assessment report (Appendix A)

This document is not intended to provide detailed assessment planning and performance guidance.

¹ https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

2. ASSESSMENT INDEPENDENCE

The MARS-E security control, CA-2(1), requires the employment of assessors or assessment teams with a CMS-defined level of independence to conduct security and privacy control assessments of the organization's information system. An assessor is independent if there is no perceived or actual conflict of interest with respect to the developmental, operational, and/or management chain associated with the information system and the determination of security and privacy control effectiveness. The AE's designated security and privacy official(s) must ensure that there is a complete separation of duties between the staff associated with the information system and the assessor or assessment team conducting the SCA. Additionally, the AE business or information system owner shall not influence the impartiality of the assessor or assessment team. To maintain the required objectivity and independence, there must be a continual evaluation of the relationships between the staff involved in the information system management and the assessors. The assessor is required to exercise professional due care, including observance of applicable professional standards.²

2.1 OPTIONS FOR INDEPENDENT ASSESSORS

In addition to contracting with an independent assessor to perform the SCA, several other options exist that could meet the independent assessor requirement for the AE. First, an AE may be able to leverage an existing state audit organization as an option for implementing an effective and independent security and privacy assessment program. An audit from a state audit organization meets the MARS-E requirement for an independent assessment if the audit incorporates the evaluation of all security and privacy control requirements specified in MARS-E. A second independent assessment option is to engage staff within the AE department to assess the MARS-E control implementation. The selected staff must have no direct responsibility for the system and/or the security or privacy posture of the system. A third option to meet the independent assessment requirement may be to leverage a current state contract, such as a contract for independent verification and validation services,³ that could be modified to include the independent assessment of MARS-E controls. The AEs may also be able to reuse existing audit reports if the audits meet the requirements of independence and the scope covers all or a portion of the MARS-E security or privacy controls; however, if only a portion of the controls are covered, assessment of the remainder of the controls is required.

2.2 PURPOSE OF THE INDEPENDENT SECURITY AND PRIVACY CONTROL ASSESSMENT

The independent SCA provides an understanding of the following:

- System compliance with MARS-E
- Underlying infrastructure's security posture
- The system and data security and privacy posture

² CMS IS Assessment Procedure, Page 3–4, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

³ For Medicaid and CHIP agencies, see 45 CFR 95.626 at <http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=aafafe72e2870be9e12ea494007c7825&ty=HTML&h=L&r=SECTION&n=45y1.0.1.1.52.4.24.14>

- Proper security configuration associated with the database or file structure storing the data
- Systems technical, managerial and organizational adherence to the organization's security and privacy program, policies, and guidance

The purpose of an SCA is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the information system. The assessment only reflects the security and privacy posture at the time of the SCA while other MARS-E controls address ongoing monitoring of control implementation.

3. ASSESSMENT PLANNING

AEs are encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of their information systems and underlying components. AEs are responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment
- Clear objectives and constraints
- Well-defined roles and responsibilities
- Scheduling that includes defined events and deliverables

During planning for the SCA, the AE develops a scope statement that is dependent upon, but not limited to, the following factors:

- System boundaries
- Known business and system risks associated with the information system
- Dependence of the system on any hierarchical structure
- System development phase
- Documented security and privacy control requirements (MARS-E)
- Assessment type
- Legislative cycle

The contract statement of work should also provide support for clarifying findings and making corrective action recommendations after the assessment.

The contract should specify that contractor staff shall execute Non-Disclosure Agreements (NDA) prior to accessing any information related to the security and privacy of the system. Requests to access information should only be considered based on a demonstration of a valid need to know, and not the position, title, level of investigation, or position sensitivity level.

4. SECURITY AND PRIVACY CONTROL ASSESSMENT METHODOLOGY

The SCA methodology described in this document originates from the standard CMS methodology⁴ used in the assessment of all CMS internal and business partner information systems.

Assessment procedures for testing each security and privacy control are in the *MARS-E Document Suite, Version 2.0 Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*⁵. A detailed assessment plan should be prepared using these security and privacy control assessment procedures. If necessary, modify or supplement the procedures to evaluate the system's vulnerability to different types of threats, including those from the insider, the Internet, or the network. The assessment methods include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls.

This assessment provides the independent assessor with an accurate understanding of the security and privacy controls in place by identifying the following:

- Application or system vulnerabilities, the associated business and system risks and potential impact
- Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system
- AE policies not followed
- Major documentation omissions and/or discrepancies

4.1 TESTS AND ANALYSES PERFORMED

The SCA includes tests that analyze the application or system and the associated infrastructure. The tests begin with high-level analyses of the application or system and increase in specificity to eventually include an analysis of each supporting component.⁶ Tests and analyses performed during an assessment should include the following:

- Security control technical testing
- Adherence to the organization's security and privacy program, policies, and guidance
- Network and component scanning
- Configuration assessment
- Documentation review
- Personnel interviews
- Observations

⁴ CMS IS Assessment Procedure, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

⁵ Regulation and Guidance, https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

⁶ A component is any element supporting the system that includes infrastructure software, hardware, and firmware.

4.1.1 Security Control Technical Testing

Typically, the assessment staff is provided user access to the system to conduct application or system security technical testing. To perform a thorough assessment of the application or system, application-specific user accounts that reflect the different user types and roles are created for the technical assessor. By providing the technical assessor with these accounts, the assessor can test application and system security controls that might otherwise not be tested. The assessors should not be given a user account with a role that would allow access to Protected Health Information (PHI) or Federal Tax Information (FTI) in any application or database.

The technical assessor attempts to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities such as buffer overflows and password compromises. The assessor must use caution to ensure no inadvertent altering of important system settings that may disable or degrade essential security or business functions. Since many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify proposed tools that pose a risk to the computing environment in the assessment plan. Furthermore, any testing that could potentially expose PII, PHI or FTI must be performed under the direct supervision of an authorized individual who is responsible for the data and can monitor the assessor's actions and take appropriate action to protect any data that is exposed.

The following list includes common test procedures and techniques of the technical assessment:

- Examination of the implemented access controls and identification and authorization techniques (e.g., log-on with easily-guessed/default passwords)
- Tests to determine if the system is susceptible to cross-site scripting (XSS), structured query language (SQL) injection, and/or other commonly exploited vulnerabilities
- Attempts to alter database management system settings
- Attempts to access hidden URLs
- Reviews of application-specific audit log configuration settings
- Determination if sensitive information is encrypted before being passed between the system and browser

4.1.2 Network and Component Scanning

In order to gain an understanding of the network and component infrastructure security posture, the SCA includes network-based scans of all in-scope network components to determine ports, protocols, and services running on each component. This provides a basis for determining the extent to which the system control implementation meets security control requirements. The results of these scans are used in conjunction with the configuration assessment.

4.1.3 Configuration Assessment

The purpose of the configuration assessment is to determine if AE security requirements are implemented correctly in the application, system, or system environmental components within the boundary of the application. The process for performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the AE security and privacy requirements

- Review access to system and databases for default user accounts
- Test firewalls, routers, systems, and databases for default configurations and user accounts
- Review firewall access control rules against the AE security requirements
- Determine consistency of system configuration with the AE-documented configuration

4.1.4 Documentation Review

The assessor must review all security and privacy documentation for completeness and accuracy. Through this process, the assessor will gain insight to determine if all controls are implemented as described. The review also augments technical control testing. For example, if the MARS-E control stipulates that the password length for the information system is required to be eight characters, the assessor must review the AE password policy or the System Security Plan (SSP) to make sure the documented password length is eight characters. During the technical configuration assessment, the assessor confirms passwords are actually configured as stated in the AE documentation. Core security documentation for review includes documents in Table 1.

Table 1: Core Security and Privacy Documentation

MARS-E Control Family	MARS-E Control Number	Document Name
Planning (PL)	PL-2: Security System Plan (SSP)	System Security Plan (SSP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	Contingency Plan Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization

4.1.5 Personnel Interviews

The assessor conducts personnel interviews to validate that security and privacy controls are implemented, staff understand and follow documented control implementations, and updated documentation is appropriately distributed to staff. The assessor interviews business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews are customized to focus on control assessment procedures that apply to individual roles and responsibilities and assure proper implementation and/or execution of security and privacy controls.

The SCA test plan identifies the designated subject matter experts (SME) interviewed. These SMEs should have specific knowledge of overall security and privacy requirements as well as a detailed understanding of the system's operational functions. The staff selected for conducting interviews should have the following roles:

- Business Owner(s)
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources Manager
- Information System Security Officer
- Privacy Program Manager
- Privacy Officer
- Media Custodian
- Network Administrator
- Program Manager
- System Administrators
- System Owner
- Training Manager

Although the initial identification of interviewees is determined when the assessment plan is prepared, additional staff may be identified as the interview process proceeds.

4.1.6 Observations

During the course of the assessment, the assessor also observes personnel behavior and the in-place, physical environmental controls, as applicable, to determine if staff follow the security and privacy policies, procedures and controls related to the physical environment are in place. For example, the assessor is required to observe:

- Processes associated with issuing visitor badges
- Requests for identification prior to visitor badge issuance
- Handling of output materials, including the labeling and discarding of output

- Equipment placement to prevent “shoulder surfing” or viewing from windows and open spaces
- Physical security associated with media protection, such as locking of telecommunication and wiring closets and access to facilities housing the system

5. SECURITY AND PRIVACY ASSESSMENT REPORTING

At the completion of the assessment, the assessor provides a security and privacy assessment report (SAR) to the AE business owner, who is then responsible for providing the report to CMS via the Collaborative Application Life Cycle Tool (CALT).

5.1 SUGGESTED REPORT STRUCTURE

The SAR structure and content of the report may be different for each AE; however, the information in the report should at a minimum provide the information noted in the next subsection and be consistent with the objectives of the assessment.

5.1.1 SAR Content

The report content should include the following information (*refer to the SAR Sample for additional details required in the report*):

- SCA methodology and testing performed
- Factual findings in accordance with the SCA tests performed
- Management information to render informed decisions regarding the application of resources and staffing to correct system weaknesses and vulnerabilities
- Remediation or compensating control recommendations

The report presents the findings of the assessment annotated in detail with the remediation recommendations for the weaknesses or deficiencies found in the information system security controls implementation. In order to reduce the risks posed to this important health care service and to protect the sensitive information of the citizens who use this service, the assessment team must assign a level of business as well as system risks to each specific finding. The assignment of business and system risk levels should follow the methodology outlined in NIST 800-30 Appendices G, H, and I.⁷ When assigning risk levels, CMS requires only three levels of granularity:

- **High** – a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, and other organizations
- **Moderate** – a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, and other organizations
- **Low** – a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, and other organizations

The CMS reporting guidance for its internal and external partners, *CMS Reporting Procedure For Information Security (IS) Assessments, March 19, 2009 Version 5.0*,⁸ provides detailed information on reporting content.

⁷ NIST 800-30 Appendices G, H and I, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

⁸ CMS IS Assessment Procedure, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

5.1.2 Sample SAR Report Structure

The SAR structure should allow the assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff. Appendix A provides a sample SAR, modeled after the SAR template used by CMS.⁹

⁹Document *Assessments - Application Finding Report Template*, <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

**APPENDIX A: SAMPLE SECURITY AND PRIVACY ASSESSMENT
REPORT (SAR)**

**<System Name>
Security and Privacy Assessment
Report**

<Date Here>

Table of Contents

1.	EXECUTIVE SUMMARY	1
1.1	<System Name> Background	1
1.2	Assessment Scope	1
1.3	Summary of Findings	2
1.4	Summary of Recommendations	3
2.	INTRODUCTION	4
2.1	Assessment Methodology	4
3.	DETAILED FINDING REPORTING	5
3.1	Tests and Analyses	5
3.1.1	Technical Testing Tools	5
3.2	Business Risk Reporting	5
3.2.1	Business Risk Level Assessment	5
3.2.2	Ease-of-Fix Assessment	5
3.2.3	Estimated Work Effort Assessment	6
4.	REPORT FINDINGS	7
5.	DOCUMENTATION LISTS	9

1. EXECUTIVE SUMMARY

The <AE> engaged <Assessor> to perform an onsite security and privacy controls assessment (SCA) of the <System Name>. <Assessor> conducted an assessment to determine:

- If the system is compliant with MARS-E
- If the underlying infrastructure supporting the system is secure
- If the system and data are securely maintained
- If proper configuration associated with the database and file structure storing the data are in place

1.1 <SYSTEM NAME> BACKGROUND

Provide a high-level overview of what the system is and what sensitive data it processes. Also briefly summarize the important, relevant facts about the system's essential business processes.

1.2 ASSESSMENT SCOPE

To determine the potential security and privacy risks to the AE, <Assessor> was tasked with providing a SCA of the <System Name> located at the {YYY Data Center (<Data center abbreviation>) in CITY NAME, STATE}. The application was assessed from <Dates of Assessment>. In accordance with the SCA Test Plan, the <Assessor> performed the following activities:

- *Interviewed selected personnel*
- *Reviewed system baselines*
- *Reviewed network component (switch/router/firewall) configurations*
- *Performed application security testing*
- *Conducted network vulnerability testing*
- *Reviewed database (DB) configuration settings*
- *Reviewed supplied security documentation*
- *Reviewed supplied privacy documentation*
- *Assessed privacy program compliance*

The following MARS-E security control families were the focus of the <System Name> assessment:

- *Access Control (AC)*
- *Awareness and Training (AT)*
- *Audit and Accountability (AU)*
- *Security Assessment and Authorization (CA)*
- *Configuration Management (CM)*
- *Contingency Planning (CP)*
- *Identification and Authentication (IA)*
- *Incident Response (IR)*
- *Maintenance (MA)*
- *Media Protection (MP)*
- *Physical and Environmental Protection (PE)*

- *Planning (PL)*
- *Program Management (PM)*
- *Personnel Security (PS)*
- *Risk Assessment (RA)*
- *System and Services Acquisition (SA)*
- *System and Communications Protection (SC)*
- *System and Information Integrity (SI)*
- *Authority and Purpose (AP)*
- *Accountability, Audit, and Risk Management (AR)*
- *Data Quality and Integrity (DI)*
- *Data Minimization and Retention (DM)*
- *Individual Participation and Redress (IP)*
- *Security (SE)*
- *Transparency (TR)*
- *Use Limitation (UL)*

1.3 SUMMARY OF FINDINGS

SUMMARY OF FINDINGS IS PROVIDED HERE:

Most findings in this document fall into the following areas:

- Access Control:
- Account Management:
- Application Security:
- Auditing and Monitoring:
- Configuration Management:
- Database Management:
- Documentation Updates:
- Identification and Authentication:
- Security Management:
- Software Maintenance:
- System and Information Integrity:
- Authority and Purpose:
- Accountability, Audit, and Risk Management:
- Data Quality and Integrity:
- Data Minimization and Retention:
- Individual Participation and Redress:
- Security:
- Transparency:
- Use Limitation:

1.4 SUMMARY OF RECOMMENDATIONS

For each finding, the Assessor has developed detailed recommendations for improvements that address the findings and the business and system risks. While all findings must be addressed, findings representing a high business risk should be mitigated or closed immediately to reduce the risk exposure. Most of the recommendations in this document fall into the following areas:

EXAMPLE FOLLOWS:

- *Block Unused Ports and Protocols:*
- *Perform Security and Privacy Monitoring:*
- *Strengthen Database Access Controls:*
- *Update Documentation:*

2. INTRODUCTION

2.1 SYSTEM SECURITY AND PRIVACY ASSESSMENT SUMMARY

The Assessor was tasked with conducting a security and privacy controls assessment (SCA) of the <System Name > to determine the overall business and system risk the system presents to the AE operations or ACA program.

Provide summary information here.

2.2 ASSESSMENT METHODOLOGY

Provide the purpose of the assessment including the controls tested and summary of the types of testing that was performed. This is obtained from the SCA test plan.

3. DETAILED FINDING REPORTING

Provides a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is explained, specific risks to the continued operations of the system are identified, the impact of each risk is analyzed, and suggested corrective actions for closing or reducing the impact of each vulnerability are presented.

3.1 TESTS AND ANALYSES

Provide details of testing and analysis performed.

3.1.1 TECHNICAL TESTING TOOLS

Provide a listing of all tools used to perform the technical test.

3.2 BUSINESS AND SYSTEM RISK REPORTING

For each weakness found, the Business and System Risk Level assessment value must be assigned to each Business and System Risk in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability.

3.2.1 BUSINESS AND SYSTEM RISK LEVEL ASSESSMENT

Management, operational, and technical vulnerabilities representing risks to the secure operation of the <System Name> are detailed as findings. Business and System Risks are technical or procedural in nature, and may result directly in unauthorized access. Each Business Risk has been assigned a Business and System Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values.

Table 1. Business and System Risk Level Definitions

Rating	Definition of Business and System Risk Rating
High	A threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals and other organizations.
Moderate	A threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals and other organizations.
Low	A threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals and other organizations.

3.2.2 EASE-OF-FIX ASSESSMENT

Each Business and System Risk is assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2 apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

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.
Moderately Difficult	<ul style="list-style-type: none"> • Remediation efforts will likely cause a noticeable service disruption. • A vendor patch or major configuration change may be required to close the vulnerability. • An upgrade to 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.
Very Difficult	<ul style="list-style-type: none"> • The high risk of substantial service disruption makes it impractical to complete the corrective action for ACA systems without careful scheduling. • 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 ACA process.
No Known Fix	<p>No known solution to the problem currently exists. The Risk may require the AE 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 ACA functions, the AE shall conduct, at a minimum, quarterly monitoring, which AE Management shall review, to validate that security incidents have not occurred</p>

3.2.3 ESTIMATED WORK EFFORT ASSESSMENT

Each Business and System Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. This value provides input for assisting in the calculating of “Resources required” in the Plan of Action & Milestones (POA&M). The definitions in Table 3 apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time [i.e., roughly three (3) days or less] is required of a single individual to complete the corrective action(s).
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. REPORT FINDINGS

The report findings provide a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is explained, specific risks to the continued operations of the system are identified, the impact of each risk is analyzed, and suggested corrective actions for closing or reducing the impact of each vulnerability are presented. The vulnerabilities are ordered in a format that will enable the business owner to develop an efficient and workable action plan to remediate all risks. The Findings are ordered first by Business Risk Level, from High Risk to Low Risk, and then by Estimated Work Effort, from Substantial to Minimal.

(Table 1. <Report Finding><Short Title> presents a table example to use for each vulnerability found during the SCA.)

Table 1. <Report Finding><Short Title>

1. <Report Finding>	<Short Title>
----------------------------------	----------------------------

Applicable Standards:

MARS-E Control Families: <Security or Privacy Control>

Control Number: <Reference>

Business Risk Level: (High Risk, Moderate Risk, or Low Risk)

<Risk Level>

Ease-of-Fix: (Easy, Moderately Difficult, Very Difficult, or No Known Fix)

<Ease of Fix>

Estimated Work Effort: (Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

<Level of Effort>

Weakness Description:

<Paragraph> <Report Date>

Finding

<Description>

Impacted components include: <hardware, software and firmware>

Failed Test Description

<Failed Condition>

Actual Test Results

<Actual Result>

Suggested Corrective Action(s):

<Recommendation>

Weakness Status:

<Status>

5. DOCUMENTATION LIST

The following table lists the documentation that <Assessor> requested prior to the onsite visit, as well as documentation provided to <Assessor> during and after the visit. The table includes the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents and the date <Assessor> received the documents. – ***This is a sample list, not all inclusive***

Table 4. Documentation Requested/Reviewed

Document Element #	Document/Information Requested	Comments
	Information System Risk Assessment	
	System Security Plan Template (For Security and Privacy Controls)	
	Contingency Plan	
	Interconnection Security Agreement	
	Contingency Plan Test	
	Configuration and Change Management Process	
	Baseline security configurations for each platform and the application within scope and baseline network configurations	
	Security Awareness and training Plan	
	Training Records	
	Incident Response (IR) Procedures	
	Privacy Impact Assessment (PIA)	