Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity (AE)

Framework for the Independent Assessment of Security and Privacy Controls

Final

Version 3.1

Version Date: June 16, 2022

Record of Changes

Version Number	Version Date	Author/Owner	A=Add M=Modify D=Delete	Description of Change	Substantive Change (Y/N)
1.0	07/2014		A	Initial draft release	
1.2	10/2015		M	Address Privacy during the IA	Y
1.9	01/2016		M	Incorporate Privacy requirements	N
2.0	03/2016		M	Incorporate comments and feedback	N
3.0	03/24/2021	Christopher Day, Abebe Feleke, Luis Effio	A, M, D	Updated the latest template, updated the footnotes with the latest references. Aligned document with the latest artifacts. Added content description and outline from the new assessor workbook. Added Risk Levels section. Rearranged document outline. Updated the required tests and assessment documents. Updated the Acronym List. Added SAW information. Added SAP section. Deleted appendix with SAR Template. Updated formatting and language.	Y
3.1	6/16/2022	Bobbie Cordle, Luis Effio	A, M	Updated to reflect that the SAP is a stand-alone document (not linked to the SAW). Updated SAR/SAP contents list. General format corrections.	N

Table of Contents

Table of Tables

1. Introduction

The Administering Entities (AEs) are custodians of sensitive information such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) 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*[1] provides an overview of the Third-Party Independent Security and Privacy Assessment Requirements and the associated Centers for Medicare & Medicaid Services (CMS) reporting process for AEs.

1.1 Framework Objectives

This framework is designed to accomplish the following objectives:

- Define assessment independence and the Third-Party Independent assessor.
- Provide a basic security and privacy control assessment methodology.
- Provide assessment planning considerations.
- Summarize security and privacy assessment reporting.

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

1.2 Requirements Background

The *Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite*[2] **Security Assessment and Authorization Control CA-2 (Security Assessments)** requires all security and privacy controls attributable to a system or application be assessed over a three-year period. Additionally, the MARS-E **Security Assessment and Authorization Control CA-2(1) (Independent Assessor)** requires that this assessment be conducted by a Third-Party Independent 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] Available at https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls

[2] Available at https://zone.cms.gov//document/minimum-acceptable-risk-standards-exchanges-mars-e-suite

2. Third-Party Independent Assessment Overview

2.1 Purpose

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 that point in time, while other MARS-E controls address ongoing monitoring of control implementation. The assessment is to be conducted on the production environment and boundaries.

The Third-Party Independent Assessment provides an understanding of the following:

- System compliance with MARS-E.
- Underlying infrastructure security posture.
- System and data security and privacy posture.
- Proper security configuration associated with the database or file structure storing the data.
- System's technical, managerial, and organizational adherence to the organization's security and privacy program, policies, and guidance.

2.2 Assessment Independence Requirements

The MARS-E **Security Assessment and Authorization Control CA-2(1) (Independent Assessor)** 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 Third-Party Independent Assessors. The assessor is required to exercise professional due care, including observance of applicable professional standards as stated in *Risk Management Handbook Chapter 4, Security Assessment and Authorization*[3].

[3] Available at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-4-Security-Assessment-and-Authorization

2.3 Alternative Options for Third-Party Independent Assessment

In addition to contracting with a Third-Party Independent Assessor to perform the SCA, the following options could meet the Independent Assessment requirement for AEs:

- 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.
- Engage staff within the AE 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.
- Leverage a current state contract, such as a contract for Independent Verification and Validation services[4], that could be modified to include the Third-Party Independent Assessment of MARS-E controls.
- 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.

3. Security and Privacy Control Assessment Methodology

Assessment procedures for testing each security and privacy control are found in the *MARS-E Document Suite.* 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 the examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls.

This assessment provides the Third-Party Independent Assessor with an accurate understanding of the security and privacy controls in place by identifying the following:

- Application or system vulnerabilities, 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 (CIA) of the system.
- AE policies not followed.

[4] For Medicaid and CHIP agencies, see 45 CFR 95.626 at https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-95/subpart-F/subject-group-ECFR8ea7e78ba47a262/section-95.626

- Major documentation omissions and/or discrepancies.

3.1 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. Tests and analyses performed during an assessment includes the following:

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

3.1.1 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 PII, PHI, or FTI in any application or database. Any testing that could potentially expose sensitive data 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.

Penetration testing is required for all Third-Party Independent Assessments. By using Penetration testing tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises, the technical assessor attempts to expose vulnerabilities associated with gaining unauthorized access to the application or system resources. 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 *Security and Privacy Assessment Plan (SAP)*[5].

[5] Available at https://zone.cms.gov/document/ae-security-and-privacy-assessment-plan-sap

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 Uniform Resource Locators (URLs)
- Reviews of application-specific audit log configuration settings
- Determination if sensitive information is encrypted before being passed between the system and browser

3.1.2 Network and Component Scanning

Network and component scanning is used to monitor, manage, and identify network elements in order to help protect the information system from possible attacks. It also helps determine the health of the network by discovering the presence of vulnerabilities. Some of the vulnerability scanning elements that should be considered are scanning patch levels, functions, ports, protocols, and services as well as improperly configured flow control mechanisms. Vulnerability scanning should be performed using the guidelines set forth in the MARS-E **Risk Assessment Control RA-5 (Vulnerability Scanning)**.

In order to gain an understanding of the network security posture, the SCA includes scans of all in-scope network components, which consists of infrastructure, application, database, and source code. This process provides a basis for determining the extent to which the system control implementation meets security control requirements. Both internal and external scanning must be performed as part of network and component scans. The results of these scans are used in conjunction with the configuration assessment.

3.1.3 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 configuration assessment should be performed against the organization's established and mandatory configuration settings as set forth in MARS-E **Configuration Management Control CM-6 (Configuration Settings)**. 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.

3.1.4 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 have a minimum of eight characters, the assessor must review the AE password policy or the MARS-E System Security and Privacy Plan (SSP) to make sure that password requirements are met. 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 below.

Table 1. Core Security and Privacy Documents

Document	MARS-E Control Family	MARS-E Control Number
System Security and Privacy Plan (SSP)	Planning (PL)	PL-2: Security System Plan
Configuration Management Plan (CMP)	Configuration Management (CM)	CM-9: Configuration Management Plan
Contingency Plan (CP)	Contingency Planning (CP)	CP-2: Contingency Plan
Contingency Plan (CP) Test Plan and Results	Contingency Planning (CP)	CP-4: Contingency Plan Testing
Incident Response Plan (IRP)	Incident Response (IR)	IR-8: Incident Response Plan
Incident Response Plan (IRP) Test Plan	Incident Response (IR)	IR-3: Incident Response Testing and Exercises
Security Awareness Training (SAT) Plan	Awareness and Training (AT)	AT-3: Role-Based Security Training
Training Records	Awareness and Training (AT)	AT-4: Security Training Records
Interconnection Security Agreement (ISA)	Security and Assessment Authorization (CA)	CA-3: System Interconnections
Plan of Action and Milestones (POA&M)	Security and Assessment Authorization (CA)	CA-5: Plan of Action and Milestones
Information Security Risk Assessment (ISRA)	Risk Assessment (RA)	RA-3: Risk Assessment
Privacy Impact Assessment (PIA) or other privacy documents	Authority and Purpose (AP)	AP-1: Authority to Collect
Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements	Authority and Purpose (AP)	AP-2: Purpose Specification
Governance documents and privacy policy	Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program

Document	MARS-E Control Family	MARS-E Control Number
Documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization	Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment

3.1.5 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 (SMEs) 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
- System Administrators
- System Owner
- Program Manager
- 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.

3.1.6 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 the security and privacy policies, procedures, and controls related to the physical environment are in place and followed by staff. 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.

3.2 Risk Levels

In order to reduce the risks posed to the system and to protect all sensitive information, the assessment team must assign a level of system risks to the findings. The assignment of system risk levels should follow the methodology outlined in National Institute of Standards and Technology (NIST) *Special Publication (SP) 800-30r1, Guide for Conducting Risk Assessments*[6], appendices G, H, and I. When assigning risk levels, CMS requires only four levels of granularity:

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

[6] Available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

4. Assessment Planning

AEs are required 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, AEs develop 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 MARS-E security and privacy control requirements.
- Assessment type.
- Legislative cycle.

The contract Statement of Work (SOW) should also provide support for clarifying findings and making corrective action recommendations after the assessment.

The contract should specify that contractor staff must execute a Non-Disclosure Agreement (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.

All information related to the assessment planning is captured in the SAP, which is to be completed prior to assessment kick-off. For submission timelines, refer to the *CMS Security and Privacy MARS-E Timelines and Artifacts List*[7].

4.1 Security and Privacy Assessment Plan

The SAP documents all testing to validate the security and privacy controls for the information system. The information included within this SAP will assist in the preparation of the *Security and Privacy Assessment Report (SAR)*[8].

[7] Available at https://zone.cms.gov/document/cms-security-and-privacy-mars-e-timelines-and-artifacts-list

[8] Available at https://zone.cms.gov/document/ae-security-and-privacy-assessment-report-template-sar

The SAP includes the following information:

- Introduction and Purpose
- Scope (system, documents, and assumptions)
- Scanning Tools and Procedures
- Test Roles
- Security and Privacy Controls Assessment Methodology
- Assessment Schedule
- Rules of Engagement (ROE)

5. Assessment Reporting

At the completion of a Third-Party Independent Assessment, the assessor provides a SAR in conjunction with the correlated Security and Privacy Assessor Workbook (SAW)[9] to the AE representative, who is then responsible for submitting the documents to CMS via the State Exchange Resource Tracking System (SERVIS). For submission timelines of all the listed documents, refer to the *CMS Security and Privacy MARS-E Timelines and Artifacts List.*

The structure and contents of both the SAR and the SAW (as described in the following subsection) must be consistent with the assessment objectives. Furthermore, all weaknesses identified in the submitted SAR and SAW need to also be captured in the associated Plan of Actions & Milestones (POA&M).

5.1 Security and Privacy Assessment Report

The SAR provides the results of the comprehensive assessment and evaluation of ACA information systems. It describes risks associated with the vulnerabilities identified during the assessment and serves as the risk summary report. The SAR allows the Assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff.

The SAR includes the following information:

- Executive Summary
- Introduction
- Scope, including components tested, documents assessed, and personnel interviews
- System Overview, including the system description and purpose
- Security and Privacy Controls Assessment Results
- Technical Testing Results, including vulnerability and configuration scan results as well as penetration test results
- Documented Exceptions, including documented risk acceptances, false positives, and known exceptions
- Detailed Assessment Results

[9] Available at https://zone.cms.gov/document/ae-security-and-privacy-assessor-workbook

- Final Assessment Findings
- Recommendations
- SAW Guidance, including general instructions and instructions for each of the main tabs.

In conjunction with the SAR, the assessor must complete the correlated tabs in SAW. The SAW provides more detailed information on the assessment results, remediation, and/or compensating control recommendations to correct system weaknesses and vulnerabilities identified through the comprehensive SCA process.

Since the SAR and the SAW are not living documents, findings should not be added or removed unless CMS' initial review of the final draft discovers deficiencies or inaccuracies that should be addressed.

Appendix A. Acronym List

AC	Access Control, a Security Control family
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AP	Authority and Purpose, a Privacy Control family
CFR	Code of Federal Regulation
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HTTPS	Hypertext Transfer Protocol Secure
Hub	ACA Data Services Hub
IP	Internet Protocol
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISRA	Information Security Risk Assessment
ISSO	Information System Security Officer
MARS-E	Minimum Acceptable Risk Standards for Exchanges
NIST	National Institute of Standards and Technology
NDA	Non-Disclosure Agreement
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action & Milestones
POC	Point of Contact
ROE	Rules of Engagement
SAP	Security and Privacy Assessment Plan
SAR	Security and Privacy Assessment Report
SAT	Security Awareness Training
SAW	Security and Privacy Assessor Workbook

SCA	Security and Privacy Control Assessment
SME	Subject Matter Expert
SOP	Senior Official for Privacy
SOW	Statement of Work
SQL	Structured Query Language
SP	Special Publication
SSP	System Security and Privacy Plan
URL	Uniform Resource Locator
XSS	Cross-Site Scripting