Centers for Medicare & Medicaid Services

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

Security and Privacy Assessment Report (SAR) for the [Administering Entity (AE Acronym) System Name (System Acronym)] System

Prepared by [Assessing Organization]

Version: [#.#]

Publication Date: [Publication Date]

Template v3.1, Dated May 5, 2022

<<Delete heading and table below before use>>

[Record of Template Changes]

Version Number	Version Date	Author/ Owner	A=Add M=Modify D=Delete	Description of Changes	Substantive Change [Y/N]
1.0	2/13/2019	LL	N/A	Document creation.	
1.1	4/6/2020	LL	M	Changed Assessment worksheet name. Updated Scope. Minor grammar corrections and formatting changes.	N
2.0	1/20/2021	CD	A, M, D	Restructured document layout. Removed tables that were added to associated Assessor Workbook. Updated instructions. Consolidated Application sections. Removed appendices. Language/grammar corrections and formatting changes.	Y
2.1	9/28/2021	Luis Effio, Danielle Andrews	A, M, D	Added SAW instructions to various sections in the document. Updated formatting and language.	Y
3.0	4/29/2022	Luis Effio, Danielle Andrews	A, M, D	Updated various sections to align with the updated SAW. Added content control boxes. Restructured document layout. Added tables to the Executive Summary. Added SAW instructions as an appendix. Added findings reference info as an appendix. Updated formatting and language.	Y
3.1	5/5/2022	Luis Effio	D	Removed findings reference info (Appendix B).	N

<<General Instructions for Completing this Report:

IMPORTANT: This page contains instructions that should be deleted prior to either hardcopy or electronic distribution of the completed draft or final SAR.

Instructions for the AEs are provided within the double arrows << … >>. Provide the required information within the brackets […], delete any remaining instructional text and unused content control boxes, and normalize the font with the surrounding text.

Although the blank template is not subject to limitations on use or disclosure from the perspective of Centers for Medicare and Medicaid Services (CMS), the completed template will contain sensitive proprietary information, and may only be disclosed as described under the terms of this SAR.>>

Report Revision History

Date	Revision Description	Version of SAR	Author
[Choose]	[Insert Revision Description]	[#.#]	[Author]

<<Add more rows as needed>>

Prepared by:

Organization Name: [Assessing Organization]
Street Address: [Insert Street Address]
Suite/Room/Building: [Insert Suite/Room/Building]
City, State Zip: [Insert Zip Code]

Prepared for:

Organization Name: [Administering Entity]
Street Address: [Insert Street Address]
Suite/Room/Building: [Insert Suite/Room/Building]
City, State Zip: [Insert Zip Code]

Table of Contents

List of Tables

Executive Summary

A Security and Privacy Control Assessment (SCA) of the [System Name or System Acronym] system was conducted between [Assessment Start Date.]-[Assessment End Date.]. The assessment was conducted in accordance with the approved Security and Privacy Assessment Plan (SAP), dated [SAP Date].

<<The assessor must provide the number of findings identified during the assessment by risk level. Those findings should align with the findings documented in the POA&M. They should derive from the results of the following:

- Vulnerability scans
- Configuration scans
- Penetration testing
- Interviews
- Control assessments
- Documentation reviews
- Additional observations>>

Table 1 below summarizes the findings identified during the assessment by risk level.

<< This information can be found in the "Findings by Risk Level" table in the SAW's "Metrics" tab.>>

Table 1. Executive Summary of Findings

Risk Level	Number of Findings
Critical	[#]
High	[#]
Moderate	[#]
Low	[#]
Total Risks	**[#]**

Table 2 below summarizes the assessment results by control assessment status.

<<The assessor must provide the total number of security and privacy controls that were assessed as well as a breakdown of controls that were met, partially met, or not met.

The data needed to complete this table can be found in the "Summary of Assessment Results by Control Family" table located in the SAW's "Metrics" tab.>>

Table 2. Summary of Control Assessment Results by Status

Control Assessment Status	Count
Met	[#]
Partially Met	[#]
Not Met	[#]
TOTAL	**[#]**

Table 3 below summarizes the results of all security scans and penetration tests, appropriately mapped to the risk level ratings.

<<The assessor must provide the total number of risks as well as a breakdown of critical, high, moderate, and low risk findings derived from the security scans and penetration test results ONLY. Priority levels are based on the impact of the identified vulnerabilities.>>

Table 3. Summary of Scan and Test Results

Risk Level	Vulnerability Scans	Configuration Scans		Penetration Test	Total
		Application Scans	Database Scans		
Critical	[#]	[#]	[#]	[#]	[#]
High	[#]	[#]	[#]	[#]	[#]
Moderate	[#]	[#]	[#]	[#]	[#]
Low	[#]	[#]	[#]	[#]	[#]
TOTAL	**[#]**	**[#]**	**[#]**	**[#]**	**[#]**

1. Introduction

The Patient Protection and Affordable Care Act (ACA) program requires use of an independent third-party assessor to perform security and privacy assessment testing and develop a SAR based on the outcomes of the assessment.

[Assessing Organization] performed a security and privacy assessment for the [System Name or System Acronym] system in accordance with the [System Name or System Acronym] SAP, version [SAP Version #], dated [SAP Date].

1.1 Applicable Laws, Regulations, and Standards

By interconnecting with the Centers for Medicare and Medicaid Services (CMS) network and the CMS information system, the AE agrees to be bound by the Administering Entity (AE) Interconnection Security Agreement (ISA) and the use of the CMS network and information system in compliance with the ISA. The following applicable laws, regulations, and standards apply:

- Office of Management and Budget (OMB) Circular A-130, Appendix I: *Responsibilities for Protecting and Managing Federal Information Resources*, July 2016.
- Title 18 of the United States Code (U.S.C.) §641, *Criminal Code: Public Money, Property, or Records*, January 2012.
- Title 18 of the United States Code (U.S.C.) § 1905, *Criminal Code: Disclosure of Confidential Information*, January 2011.
- Health Insurance Portability and Accountability Act (HIPAA) of 1966 (Public Law [PL] 104-191), August 1996.
- The Patient Protection and Affordable Care Act of 2010 (ACA) (PL 111-148), March 2010.
- The ACA (PL 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (PL 111-152), March 2010.
- Department of Health and Human Services (HHS) Regulation 45 Code of Federal Regulation (C.F.R.) §155.260, *Privacy and Security of Personally Identifiable Information (PII)*, October 2014.
- Department of Health and Human Services (HHS) Regulation 45 Code of Federal Regulation (C.F.R.) §155.280, *Oversight and Monitoring of Privacy and Security Requirements*, October 2015.
- The Privacy Act of 1974, Title 5 of the Code of Federal Regulation (U.S.C.) §552a. System of Records Notice citation: "Health Insurance Exchanges Program", Title 78 of the Federal Register 8538, February 2013.
- Department of Health and Human Services (HHS) Title 45 C.F.R. §155.260(b) – *Privacy and Security of Personally Identifiable Information (PII) for Exchange Functions*, October 2014.

- Social Security Act, Section 1943(b) (as added by section 2201 of the ACA (PL 111-148), March 2010.
- The Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite.

<<List additional state laws, regulations, and standards as necessary.>>

1.2 Purpose

This SAR provides the [AE Name or AE Acronym] Information System Security Officer (ISSO), Senior Official for Privacy (SOP), and Authorizing Officials (AOs) with the results of the assessment completed for the [System Name or System Acronym] system. The report describes risks associated with the vulnerabilities identified during the [System Name or System Acronym] system independent security and privacy assessment and serves as the risk summary report, as referenced in the *Framework for Independent Assessment of Security and Privacy Controls*[1] and the *Information Security and Privacy Continuous Monitoring (ISCM) Guide for Administering Entity (AE) Systems*[2], developed using guidance from the *Minimum Acceptable Risk and Standards (MARS-E)* Document Suite[3].

2. Scope

The assessor analyzed all assessment results to provide the [AE Name or AE Acronym] ISSO, SOP, and the AOs with an assessment of the security and privacy controls that safeguard the Confidentiality, Integrity, and Availability (CIA) of data hosted by the system as described in the [System Name or System Acronym] System Security and Privacy Plan (SSP).

This SAR is required for [Reason for the Assessment]. It presents the results of a security and privacy assessment of the [System Name or System Acronym] system and is provided to support the [AE Name or AE Acronym]'s program goals, efforts, and activities necessary to achieve compliance with the necessary security and privacy requirements.

[AE Name or AE Acronym] engaged [Assessing Organization] to perform an onsite SCA of the [System Name or System Acronym] system in order to determine if:

- The system is compliant with MARS-E [#.#];
- The underlying infrastructure supporting the system is secure;
- The system and data are securely maintained; and
- Proper configuration associated with the database and file structure storing the data is in place.

The SCA consisted of system components and documentation reviews.

[1] Available at https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls

[2] Available at https://zone.cms.gov/document/information-security-and-privacy-continuous-monitoring-guide-administering-entity-systems

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

2.1 Components Tested

<<Provide a list of all individual components that were tested in Table 4 below indicates all individual components that were tested during this assessment.
Table 4. The listed components should be consistent with those addressed in the SSP. For the components that were addressed in the SSP but not tested, add an explanation in the Comments section of the table. Include additional components as necessary.

Examples:

- Operating system, version #
- Database, version #
- Application, version #
- URL
- System subcomponent

Security and privacy documentation will be reviewed for completeness and accuracy through the assessment process. The assessor will gain insight to determine if all controls are implemented as described. The assessor's review also augments technical control testing.>>

Table 4 below indicates all individual components that were tested during this assessment.

Table 4. Tested Components

Components planned to be tested	Were components tested?	Comments
[Insert component]	[Choose an item]	[Insert comment]
[Insert component]	[Choose an item]	[Insert comment]
[Insert component]	[Choose an item]	[Insert comment]
[Insert component]	[Choose an item]	[Insert comment]

<<Add more rows as needed.>>

2.2 Documents Assessed

The following documents were assessed:

<<Choose all assessed documents. Delete all documents not submitted/reviewed. Convert bullets that remain to black font.>>

- Business agreement with Data Use Agreement (DUA)
- Configuration Management Plan (CMP)
- Contingency Plan and test results
- Plan of Action and Milestones (POA&M)

- System Security Plan (SSP) (final)
- Incident Response Plan (IRP) and incident/breach notification and test plan
- Privacy Impact Assessment (PIA) and other privacy documentation, including, but not limited to, privacy notices as well as agreements to collect, use, and disclose Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), and privacy act statements
- Security Awareness Training (SAT) plan and training records;
- Interconnection Security Agreement (ISA)
- Information Security Risk Assessment (ISRA)
- Governance documents and privacy policy
- Documentation describing the organization's privacy risk assessment process and documentation of privacy risk assessments performed by the organization

<<List additional assessed documents as necessary.>>

2.3 Personnel Interviewed

The assessor interviewed business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews were customized to focus on control assessment procedures that apply to individual roles and responsibilities and to assure proper implementation and/or execution of security and privacy controls.

<<Using the table below, remove/add rows as necessary and populate the required fields.>>

Table 5 below indicates the personnel selected to be interviewed.

Table 5. Personnel Interviewed

Title	Name of Person	Date of Interview	Comments
Business Owner(s)	[Insert name]	[Choose date]	[Insert comments]
Application Developer	[Insert name]	[Choose date]	[Insert comments]
Configuration Manager	[Insert name]	[Choose date]	[Insert comments]
Contingency Planning Manager	[Insert name]	[Choose date]	[Insert comments]
Database Administrator	[Insert name]	[Choose date]	[Insert comments]
Data Center Manager	[Insert name]	[Choose date]	[Insert comments]
Facilities Manager	[Insert name]	[Choose date]	[Insert comments]
Firewall Administrator	[Insert name]	[Choose date]	[Insert comments]

Title	Name of Person	Date of Interview	Comments
Human Resources Manager	[Insert name]	[Choose date]	[Insert comments]
Information System Security Officer	[Insert name]	[Choose date]	[Insert comments]
Privacy Program Manager	[Insert name]	[Choose date]	[Insert comments]
Privacy Officer	[Insert name]	[Choose date]	[Insert comments]
Media Custodian	[Insert name]	[Choose date]	[Insert comments]
Network Administrator	[Insert name]	[Choose date]	[Insert comments]
Program Manager	[Insert name]	[Choose date]	[Insert comments]
System Administrators	[Insert name]	[Choose date]	[Insert comments]
System Owner	[Insert name]	[Choose date]	[Insert comments]
Training Manager	[Insert name]	[Choose date]	[Insert comments]

<<Add more rows as needed.>>

3. System Overview

3.1 System Description

<<In this subsection, insert a general description of the information system. The description should align with the description found in the SSP. The description in this subsection may differ only if additional information is included that is not available in the SSP or if the description in the SSP is not accurate.>>

[Insert description]

3.2 Purpose of System

<<Insert the purpose of the information system. The purpose must align with the purpose provided in the SSP.>>

[Insert purpose]

4. Security and Privacy Controls Assessment Results

The "Security and Privacy Controls" tab of the AE Security and Privacy Assessor Workbook (SAW)[4] details the security controls assessment results for each of the controls being assessed.

4.1 Security and Privacy Control Assessment Results by Control Family

Table 6 below summarizes the security and privacy controls assessment results by control family.

<<The assessor must provide the total number of security and privacy controls that were assessed as well as a breakdown of controls that were met, partially met, or not met for each control family.

The table below includes the results from the MARS-E assessment requirements as described in the System Security and Privacy Plan (Volume IV of MARS-E 2.0 and volume II of MARS-E 2.2).

The data needed to complete this table can be found in the SAW's "Metrics" tab.>>

Table 6. Summary of Assessment Results by Control Family

Security and Privacy Control Family	Met	Partially Met	Not Met	Total
AC – Access Control	[#]	[#]	[#]	[#]
AT – Awareness and Training	[#]	[#]	[#]	[#]
AU – Audit and Accountability	[#]	[#]	[#]	[#]
CA – Security Assessment and Authorization	[#]	[#]	[#]	[#]
CM – Configuration Management	[#]	[#]	[#]	[#]
CP – Contingency Planning	[#]	[#]	[#]	[#]
IA – Identification and Authentication	[#]	[#]	[#]	[#]
IR – Incident Response	[#]	[#]	[#]	[#]
MA – Maintenance	[#]	[#]	[#]	[#]
MP – Media Protection	[#]	[#]	[#]	[#]
PE – Physical and Environmental Protection	[#]	[#]	[#]	[#]
PL – Planning	[#]	[#]	[#]	[#]
PM – Program Management	[#]	[#]	[#]	[#]
PS – Personnel Security	[#]	[#]	[#]	[#]
RA – Risk Assessment	[#]	[#]	[#]	[#]
SA – System and Services Acquisition	[#]	[#]	[#]	[#]
SC – System and Communications Protection	[#]	[#]	[#]	[#]
SI – System and Information Integrity	[#]	[#]	[#]	[#]

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

Security and Privacy Control Family	Met	Partially Met	Not Met	Total
AP – Authority and Purpose	[#]	[#]	[#]	[#]
AR – Accountability, Audit, and Risk Management.	[#]	[#]	[#]	[#]
DI – Data Quality	[#]	[#]	[#]	[#]
DM – Data Minimization and Retention	[#]	[#]	[#]	[#]
IP – Individual Participation and Redress	[#]	[#]	[#]	[#]
SE – Security	[#]	[#]	[#]	[#]
TR – Transparency	[#]	[#]	[#]	[#]
UL – Use Limitation	[#]	[#]	[#]	[#]
TOTAL	**[#]**	**[#]**	**[#]**	**[#]**

Progress on satisfying any previously identified weaknesses must be actively monitored. Details of this review, including any management comments, are provided in the SAW.

5. Technical Testing Results

5.1 Vulnerability Scan Results

<<Upload a file/zip file containing the detailed vulnerability scan results generated by the scanner to the AE's folder in the State Exchange Resource Virtual Information System (SERVIS). Provide the name of that file/zip file below. The file/zip file can be no more than 40MB. Use the naming convention found in the CMS SERVIS Artifact Submission Procedures to properly name the file/zip file.>>

Vulnerability scans include scans of operating systems, networks, routers, firewalls, Domain Name System (DNS), domain servers, Network Information Security (NIS) masters, and other devices that keep the network running. These scans can include both physical and virtual hosts and devices. For the remaining inventory, the assessor performed a manual review of configuration files to analyze for existing vulnerabilities.

The following scanning tools were used to scan the [System Name or System Acronym] system's infrastructure:

Table 7. Vulnerability Scanning Tools Information

Scanner Name	Vendor	Version #
[Scanner Name]	[Vendor]	[Version #]

<<Add more rows as necessary.>>

The authenticated vulnerability scan results have been uploaded to SERVIS with the following file name(s):

- [Insert file name]

5.2 Configuration Scan Results

Configuration scans include software flaws, missing patches, malware, and misconfigurations across all operating systems, devices, applications, and databases.

5.2.1 Applications

<<Upload a file/zip file containing the detailed application scan results generated by the scanner to the AE's folder in the State Exchange Resource Virtual Information System (SERVIS). Provide the name of that file/zip file below. The file/zip file can be no more than 40MB. Use the naming convention found in the CMS SERVIS Artifact Submission Procedures to properly name the file/zip file.>>

The following scanning tools were used to scan the [System Name or System Acronym] system's applications:

Table 8. Applications Scanning Tools Information

Scanner Name	Vendor	Version #
[Scanner Name]	[Vendor]	[Version #]

<<Add more rows as necessary.>>

The authenticated application scan results have been uploaded to SERVIS with the following file name(s):

- [Insert file name]

5.2.2 Databases

<<Upload a file/zip file containing the detailed database scan results generated by the scanner to the AE's folder in the State Exchange Resource Virtual Information System (SERVIS). Provide the name of that file/zip file below. The file/zip file can be no more than 40MB. Use the naming convention found in the CMS SERVIS Artifact Submission Procedures to properly name the file/zip file.>>

The following scanning tools were used to scan the [System Name or System Acronym] system's databases:

Table 9. Databases Scanning Tools Information

Scanner Name	Vendor	Version #
[Scanner Name]	[Vendor]	[Version #]

<<Add more rows as necessary.>>

The authenticated database scan results have been uploaded to SERVIS with the following file name(s):

- [Insert file name]

5.3 Penetration Test Results

<< Export results from the penetration test scan tool to the "Pen Test Results" tab of the SAW,

OR

Upload a file/zip file containing the detailed pen test results to the AE's folder in the State Exchange Resource Virtual Information System (SERVIS). Provide the name of that file/zip file in the "Pen Test Results" tab of the SAW. The file/zip file can be no more than 40MB. Use the naming convention found in the CMS SERVIS Artifact Submission Procedures to properly name the file/zip file.>>

The scope of this assessment was limited to the [System Name or System Acronym] system's solution, including [List components as documented in the SSP and Penetration Test Plan]. The assessor conducted testing of the [System Name or System Acronym] system activities from [City, State] via an attributable internet connection.

The detailed Pen Test results can be found Choose an item.

<<Insert SERVIS Files name(s) in bullet format, if applicable.>>

6. Documented Exceptions

6.1 Documented Risk Acceptances

Risk Acceptance is only considered in those cases where all reasonable mitigation options have been exhausted. For any accepted risk, the risk has been deemed acceptable because it fit within the AE's risk tolerance level.

Risk acceptances for the [System Name or System Acronym] system are documented in the "Documented Exceptions" tab of the SAW.

6.2 False Positives

False positives occur when the scanner can access only a subset of the required information, which prevents it from accurately determining whether a vulnerability exists. To help reduce the number of false positives, scanners must be configured with the appropriate credentials.

False positive results for all layers of the [System Name or System Acronym] system are documented in the SAW's "Documented Exceptions" tab.

6.3 Known Exceptions

Certain vulnerabilities may not be considered necessary and thus can be exempted from being reported for a number of reasons, including but not limited to the following:

- The vulnerability does not apply to runtime or cannot be exploited.
- A suggested fix will break a chain of dependencies.
- There is no fix for a particular vulnerability and a temporary alternative security strategy has been identified.

Known exceptions for the [System Name or System Acronym] system are documented in the SAW's "Documented Exceptions" tab.

7. Detailed Assessment Results

All individual weaknesses identified during the assessment are listed in the "Detailed Assessment Results" tab of the SAW. This is comprised of all weaknesses as identified in Table 2 and Table 3 of this report.

<<The assessor must provide the number of individual weaknesses identified during the assessment by risk level. They should derive from the results of the following:

- Vulnerability scans
- Configuration scans
- Penetration testing
- Interviews
- Control assessments
- Documentation reviews
- Additional observations>>

Table 10 below summarizes the findings identified during the assessment by risk level.

<< This information can be found in the SAW's "Metrics" tab.>>

Table 10. Individual Weaknesses by Risk Level

Risk Level	Number of Weaknesses
Critical	[#]
High	[#]
Moderate	[#]
Low	[#]
Total Risks	**[#]**

8. Final Assessment Findings

All findings identified during the assessment as well as the justification for consolidation (when applicable) are listed in the SAW's "Final Assessment Findings" tab.

<<Provide a narrative summary of the findings identified during the assessment.

For example: "Many of the findings fall into the Access Control (AC) family due to the misconfiguration of the database and web application services, and overdue account reviews..."

[Insert summary]

9. Recommendations

<< While all findings must be addressed, findings representing a critical or high business risk should be mitigated or closed immediately to reduce the risk exposure. The following example list of findings should be modified based on the SCA results:

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

Provide a summary of recommendations grouped by control families, if possible. Identify which corrective actions can mitigate large groups of findings.

For example: "The Access Control (AC) and most of the Configuration Management (CM) findings can be remediated if the database is upgraded to the latest version of the software, and necessary hot fixes and patches are applied.">>

For each finding, the assessor developed detailed recommendations for improvements that address the findings and the business and system risks. Most of the recommendations fall into the following areas:

[Insert recommendations]

Appendix A. SAW Guidance

This Appendix provides details that align to the following SAW tabs:

- General Instructions
- Security and Privacy Controls
- Detailed Assessment Results
- Final Assessment Findings
- Pen Test Results
- Documented Exceptions

General Instructions

The SAW's "General Instructions" tab offers guidance on which tabs need completed for each type of assessment:

- Annual Self-Assessment:
  - Security and Privacy Controls
- Third-Party Independent Assessment:
  - Security and Privacy Controls
  - Detailed Assessment Results
  - Final Assessment Findings
  - Pen Test Results
  - Documented Exceptions

The guidance also offers detailed instructions on how to complete the "Security and Privacy Controls" tab. The instructions provide a step by step walk through of filtering requirements based on the assessment type and timeline.

Security and Privacy Controls

Below are the descriptions for each of the fillable columns in the "Security and Privacy Controls" tab.

1. **Administering Entity**: Enter the state, territory, or name of the administering entity.
2. **System Name**: Enter the system name.
3. **System Acronym**: Enter the system acronym.
4. **Report Date**: Enter the date of SAW finalization.
5. **Attestation Year**: This column identifies the Annual Attestation year(s) for the controls being assessed in addition to supplemental controls required by CMS (if any). Follow the instructions in the "General Instructions" tab to select the controls being assessed.
6. **Examine:** Identify artifacts and processes examined for each control.
7. **Interview**: Identify the personnel or the role of the individual interviewed to confirm implementation of each control.
8. **Test**: Identify methods and objects used to test each control. If automated tools were utilized for the assessment, identify which tools were utilized.

9. **Pass/Fail**
   Applicable for Examine, Interview, and Test:
   a. Pass: If system provides control(s) that mitigate(s) vulnerability/threat.
   b. Fail: If system does NOT provide control(s) that mitigate(s) vulnerability/threat.
   c. N/A - The requirement is not applicable.
10. **Control Results**
   a. Met - The requirement has been completely satisfied.
   b. Partially Met - The requirement has been partially satisfied. Comments are required.
   c. Not Met - The requirement has not been satisfied. Comments are required.
   d. N/A - The requirement is not applicable. Comments are required.
11. **Comments**: Any additional details necessary to clarify weakness information, status, and/or traceability must be documented in this field. If the solution does not fully address each control requirement, document any compensating controls in place that reduce the residual risk.

Detailed Assessment Results

Use the SAW's "Detailed Assessment Results" tab to provide a descriptive analysis of each of the individual weaknesses identified through the comprehensive SCA process. All weaknesses identified during the assessment, including those discovered through scanning and penetration testing, should be addressed.

Weaknesses that were discovered but remediated during the assessment process still need to be included indicating that remediation has occurred.

Below are the descriptions for each of the columns in the "Detailed Assessment Results" tab.

1. **Weakness Reference Number**: Each weakness has a sequential row number included to provide easy reference for briefings and cross-referencing.
2. **POA&M Identifier**: Identify the corresponding POA&M Identifier, which is a unique number assigned to each POA&M finding that is used to track the weakness. The format: [System name or acronym]_[Quarter (A, B C, or D)]_[Fiscal Year the weakness was first recorded]_[a sequence number] (e.g., System1_A_2022_4)
3. **Risk Level**: Risk level of weakness is identified in the SAR, Audit or Review. The assignment of risk levels should follow the methodology outlined in NIST 800-30 Appendices G, H, and I. In assigning risk levels, CMS requires 4 levels of granularity: Critical, High, Moderate, and Low.

Rating	Definition of Risk Rating
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.

Rating	Definition of Risk Rating
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the CIA 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 CIA of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment.

4. **Control Details/CVE/Plugin ID**: Input the Control Details/CVE/Plugin ID. Multiple may be entered if applicable.
5. **Affected System**: Document the system, URL, IP address, etc., affected by the weakness. For example: “SQL Server: master” or “127.0.0.1”
6. **Weakness Description**: Detailed description of the vulnerability or risk identified. This information may be found in the SAR or other security audit type report.
7. **Failed Test Description**: Documents the control’s weakness that resulted in the finding. This description provides specific information from the security and privacy policy, requirements, guidance, test objective, or published industry best practices that was not provided with the controls implementation.
8. **Actual Test Results**: Provides specific information on the observed failure of the test objective, policy, or guidance. This may also contain output from a test performed on the system revealing non-compliance.

Final Assessment Findings

Use the SAW’s “Final Assessment Findings” tab to provide a descriptive analysis of the findings (individual and consolidated) identified through the comprehensive SCA process. All findings identified during the assessment, including those discovered through scanning and penetration testing, should be addressed.

Below are the descriptions for each of the columns in the “Final Assessment Findings” tab.

1. **POA&M Identifier**: Find this in the "Detailed Assessment Results" tab, column B.
2. **Weakness Reference Number(s)**: Find this information in the “Detailed Assessment Results” tab, Column A. Multiple numbers may be entered when applicable.
3. **Control Family**: Input the control family that best signifies the origin of the finding. Multiple may be entered if applicable. For example, “AC” or, if more than one control, “AC, CA”.
4. **Control Details**: Input the control number that best signifies the origin of the finding. Multiple may be entered if applicable. For example, “AC-3” or, if more than one control, “AC-2 (4), AC-3, CA-7”.
5. **Source**: Provide the type of review and the date on which the review was conducted or published. If it represents a repeat finding, each source in which the weakness was identified must be documented.
6. **Justification for Consolidation**: Provide the justification for consolidation of multiple weaknesses into one finding. If not applicable, note "N/A".

7. **Risk Level**: Risk level of weakness is identified in SAR, Audit or Review. The assignment of risk levels should follow the methodology outlined in NIST 800-30 Appendices G, H, and I. In assigning risk levels, CMS requires 4 levels of granularity: Critical, High, Moderate, and Low.

   Note: If the finding is comprised of several individual weaknesses, use the weakness with the highest risk level to determine the overall risk level.

Rating	Definition of Risk Rating
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 CIA 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 CIA of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment.

8. **Remediation Status:** Provide the current remediation status (e.g., open, completed, delayed, or risk-accepted).
9. **Recommendations**: Provide the recommended actions to resolve the finding. The assessor provides these suggestions to present guidance on a potential fix.

Penetration Test Results

If using the SAW to provide penetration test results, export results from the penetration test scan tool to the "Pen Test Results" tab in a suitable format.

Documented Exceptions

Documented Risk Acceptances

Provide all documented risk acceptances for the system in the SAW's "Documented Exceptions" tab. Ensure that the required Risk Acceptance Form for each accepted risk has been submitted to SERVIS and include the date that the form was submitted in the SAW.

Refer to the Risk Acceptance Guidance for the Administering Entity (AE) Information Systems on zONE for instructions and when and how to submit the Risk Acceptance Form, also found on zONE.

False Positives

Provide false positive results for ALL layers of the system in the SAW's "Documented Exceptions" tab.

For each false positive reported, add the type and an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positives reported, identify each in separate rows. Add as many rows as necessary.

Known Exceptions

Provide all known exceptions for the system in the SAW's "Documented Exceptions" tab.

Appendix B. Acronym List

AC	Access Control, a Security Control family
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AO	Authorizing Officials
AP	Authority and Purpose, a Privacy Control family
AR	Accountability, Audit, and Risk Management, a Privacy Control family
AT	Awareness and Training, a Security Control family
AU	Audit and Accountability, a Security Control family
CA	Security Assessment and Authorization, a Security Control family
C.F.R.	Code of Federal Regulation
CIA	Confidentiality, Integrity, and Availability
CM	Configuration Management, a Security Control family
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Planning, a Security Control family
DI	Data Quality, a Privacy Control family
DM	Data Minimization and Retention, a Privacy Control family
DNS	Domain Name System
DUA	Data Use Agreement
FISMA	Federal Information Security Management Act
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IA	Identification and Authentication, a Security Control family
IP	Individual Participation and Redress, a Privacy Control family
IR	Incident Response, a Privacy Control family
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCM	Information Security and Privacy Continuous Monitoring
ISRA	Information Security Risk Assessment

ISSO	Information System Security Officer
MA	Maintenance, a Privacy Control family
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MP	Media Protection, a Privacy Control family
OMB	Office of Management and Budget
PDF	Portable Document Format
PE	Physical and Environmental Protection, a Privacy Control family
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Planning, a Security Control family
PL	Public Law
PM	Program Management, a Privacy Control family
POA&M	Plan of Action & Milestones
PS	Personnel Security, a Privacy Control family
RA	Risk Assessment, a Security Control family
SA	System and Services Acquisition, a Privacy Control family
SAP	Security and Privacy Assessment Plan
SAR	Security and Privacy Assessment Report
SAT	Security Awareness Training
SC	System and Communication Protection, a Privacy Control family
SCA	Security and Privacy Controls Assessment
SE	Security, a Privacy Control family
SERVIS	State Exchange Resource Virtual Information System
SI	System and Information Integrity, a Privacy Control family
SOP	Senior Official for Privacy
SSP	System Security and Privacy Plan
TR	Transparency, a Privacy Control family
UL	Use Limitation, a Privacy Control family
URL	Uniform Resource Locator
U.S.C.	United States Code