



Security Risk Assessment Tool v3.4

User Guide

DISCLAIMER

The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights (OCR) Health Information Privacy website at: www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

Updated: September 5, 2023

Contents

WHAT'S NEW IN VERSION 3.4.....	3
BACKGROUND.....	4
SRA Tool Overview	4
What to expect with the SRA Tool	4
End User Hardware Requirements.....	6
Download Instructions	7
USING THE TOOL.....	8
Starting a New Assessment.....	8
Continuing an Assessment	9
Saving Assessment Progress	10
Add Practice Information	10
Add/Edit Asset Information	11
Upload Asset Template (Bulk Operations).....	12
Add/Edit Vendor Information	13
Upload Vendor Template (Bulk Operations).....	14
Link Additional Documentation	16
Glossary Terms	17
Completing the Assessment.....	18
Threat & Vulnerability Rating.....	19
Section Summary	20
Assessment Summary	21
Risk Report	22
Detailed Report	23
Flagged Report	24
Remediation Report	25
Saving & Exporting	26
Version Information	26
SRA Tool Version	27
Content Version.....	27
Content Version Out-of-Date warning	27
SRA TOOL EXCEL WORKBOOK.....	28
FREQUENTLY ASKED QUESTIONS [FAQ'S].....	29

What's new in version 3.4

SRA Tool version 3.4 includes a variety of new enhancements and bug fixes based on user feedback from previous versions.

- ▲ New features and updates to SRA Tool Version 3.4 include:
 - Inclusion of additional HICP references
 - Interactive glossary of terms
 - Remediation Report
 - Bug fixes and stability improvements

Background

The Security Risk Assessment Tool (SRA Tool) is designed to help covered entities and business associates that handle patient data identify and assess risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information (PHI) in their environment. The HIPAA Security Rule requires health care providers, health plans and business associates to conduct risk analyses and implement technical, physical, and administrative safeguards to protect Electronic Protected Health Information (ePHI). The Office for the National Coordinator for Health IT worked together with the Office for Civil Rights, which enforces the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), to develop this tool to assist providers and business associates with meeting their responsibility to protect ePHI.

The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations. Through use of the SRA Tool organizations can assess and document the information security risks to ePHI in their organizations.

We hope you find this tool helpful as you work towards improving the privacy protections and security of your organization and its compliance with the HIPAA Security Rule's risk analysis requirement. Please remember that this is only a tool to assist an organization with its review and documentation of its risk assessment, and therefore it is only as useful as the work that goes into performing and recording the risk assessment process. Once you have assessed your security risks using the tool, you may need to take appropriate steps to remediate any areas found wanting. Use of this tool does not mean that your organization is compliant with the HIPAA Security Rule or other federal, state or local laws and regulations. It does, however, assist organizations with the HIPAA Security Rule requirement to conduct periodic security risk assessments.

SRA Tool Overview

Note: *The SRA Tool runs on your computer. It does not transmit information to the Department of Health and Human Services, The Office of the National Coordinator for Health IT, or The Office for Civil Rights.*

The SRA tool is available for download on ONC's website, HealthIT.gov. The SRA tool is a Windows-based application that can be installed locally on the user's computer. With a wizard-based workflow and section summary reporting, users receive feedback and progress indicators as they work through the security risk assessment for their organization. It supports multiple user accounts and a collaborative file sharing. In addition, it allows organizations to track assets, current encryption levels for assets, business associates, and associated satisfactory assurances or risks pertaining those businesses. All user entered data is saved locally in a secure format (only accessible for decryption by the SRA Tool application).

The SRA Tool is a software application available for download from the ONC's HealthIT.gov website. It is available at no cost and can be used with Windows 7/8/9/10/11 operating systems. The SRA Tool installs to the Program Files directory [Administrator privileges are required to install].

What to expect with the SRA Tool

The SRA Tool guides covered entities and business associates (regulated entities) through a series of questions based on the standards and implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues. There are currently 7 sections of content covering these areas:

- Section 1: Security Risk Assessment (SRA) Basics (security management process)
- Section 2: Security Policies, Procedures, & Documentation (defining policies & procedures)

SRA Tool v3.4 User Guide

- Section 3: Security & Your Workforce (defining/managing access to systems and workforce training)
- Section 4: Security & Your Data (technical security procedures)
- Section 5: Security & Your Practice (physical security procedures)
- Section 6: Security & Your Vendors (business associate agreements and vendor access to PHI)
- Section 7: Contingency Planning (backups and data recovery plans)

The sources of information used to support the development of the SRA Tool questionnaires include the following:

- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication 800-66
- NIST Special Publication 800-53
- NIST Special Publication 800-53A
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- NIST Cybersecurity Framework
- Health Industry Cybersecurity Practices (HICP) Technical Volume 1

The SRA Tool takes you through each section by presenting a question about your organization's activities. Your answers will show you if you should take corrective action for that item or continue with your current security activities. If corrective action is suggested, the tool provides guidance on the related HIPAA Rule requirement or security reference and suggestions on how to improve. Following each assessment section, the tool prompts you to select applicable vulnerabilities and rate associated threats in terms of likelihood and impact to determine your risk level. The tool also provides section summaries with your results for each subset of questions.

The SRA Tool provides resources to help users...

- Understand the context of the question
- Consider the potential impacts to ePHI in your environment
- Identify relevant security references (e.g., the HIPAA Security Rule)

You can document your answers and comments directly into the SRA Tool in the "Details" section on individual questions or the "Additional Information" in the section summary. In addition, a "Remediation Plan" section has been added to version 3.4 to aid in documenting plans to mitigate risks identified when completing the assessment. The tool serves as your local repository for the information. Organizations can also attach supporting documentation of activities taken during the risk assessment process - for example, activities demonstrating how technical vulnerabilities are identified.

The HIPAA Security Rule's risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of an organization's ePHI, including ePHI on all forms of electronic media. The questions presented by the SRA Tool are designed to help organizations identify risks to ePHI common to small and medium sized regulated entities. Risks that are known to a regulated entity, but not identified by the SRA Tool should nonetheless be identified, assessed, and documented to ensure the risk assessment is accurate and thorough for your organization. Additionally, if responses to questions in the tool represent risks in the aggregate, organizations should ensure that tool responses include sufficient detail or that supplemental documentation is maintained supporting aggregate risk determinations. Further, as a point-in-time questionnaire-based tool, risks specific to certain technologies or of specific technical vulnerabilities may not be identified by the tool. Regulated entities should account for such risks with supplemental documentation

as necessary. If, after completing all of the questions in the SRA Tool, threats and vulnerabilities are known but are unaccounted for in the SRA Tool (i.e., a particular threat or vulnerability was not listed in the tool or the questions were not relevant to a risk area specific and known to the organization), the organization must either 1) document the unaccounted threats and vulnerabilities and assess the risks posed to ePHI in the most appropriate place within the SRA Tool, or 2) document the unaccounted threats and vulnerabilities and assess the risks posed to ePHI as part of a separate document to supplement the SRA Tool. Such documentation can be attached to the tool using the tool's the add document functionality.

Completing a risk assessment requires a time investment. At any time during the risk assessment process, you can pause to view your current results. The results are available in a color-coded graphic view and printable format.

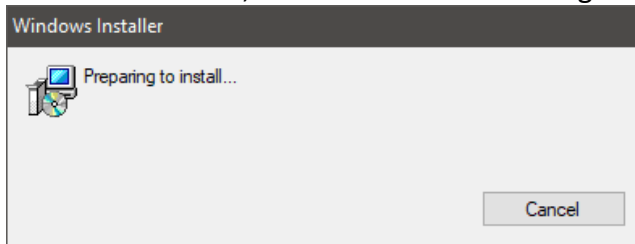
Need Help? *Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future. *Persons using assistive technology may not be able to fully access information in this file. For assistance, contact ONC at PrivacyAndSecurity@hhs.gov.*

End User Hardware Requirements

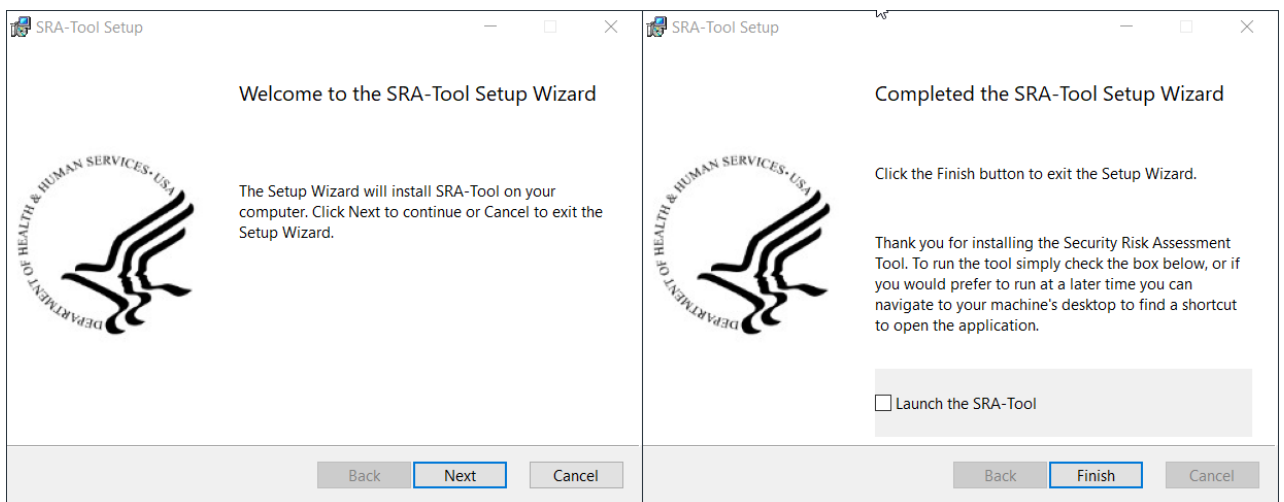
- Windows 7/8/10/11
- 2 GHz Pentium processor or better
- 2 GB RAM or more
- System type: 64-bit Operating System
- 1024 x768 screen resolution or better

Download Instructions

1. Download the tool from the HealthIT.gov website
 - a. <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment>
2. Once downloaded, run the executable to begin installation to your computer.



3. You will see a status indicator of the installation progress while the tool is being installed on your machine.

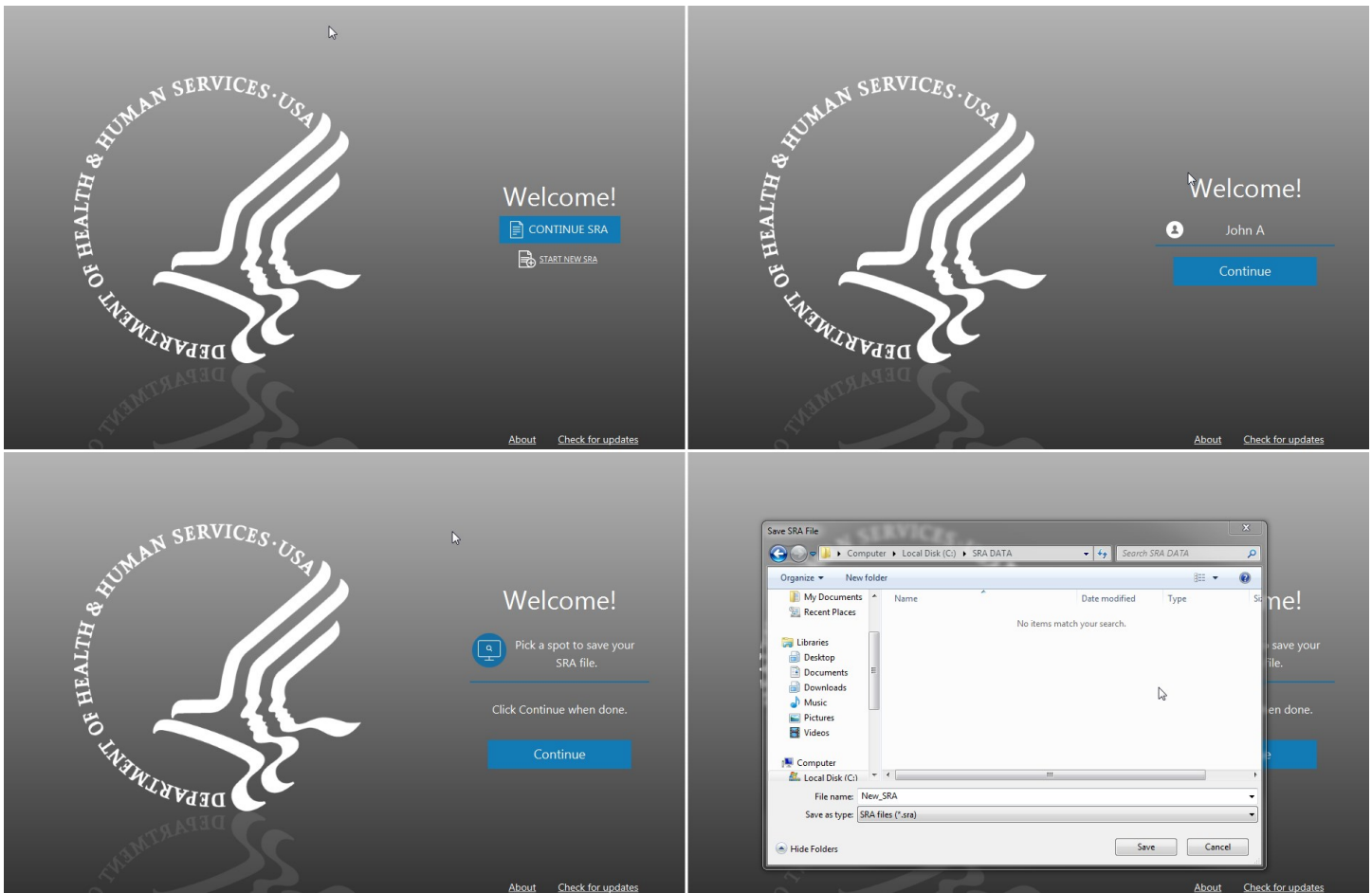


4. When installation is complete, click "Finish" in the installation setup wizard.
5. Then locate and double click the SRA-Tool icon on your desktop to begin using the tool.

Note: The SRA Tool v3.4 installs to the Program Files directory which requires administrative privileges. If you are having difficulty completing the installation of the tool, you may need to check with your administrator.

Using The Tool

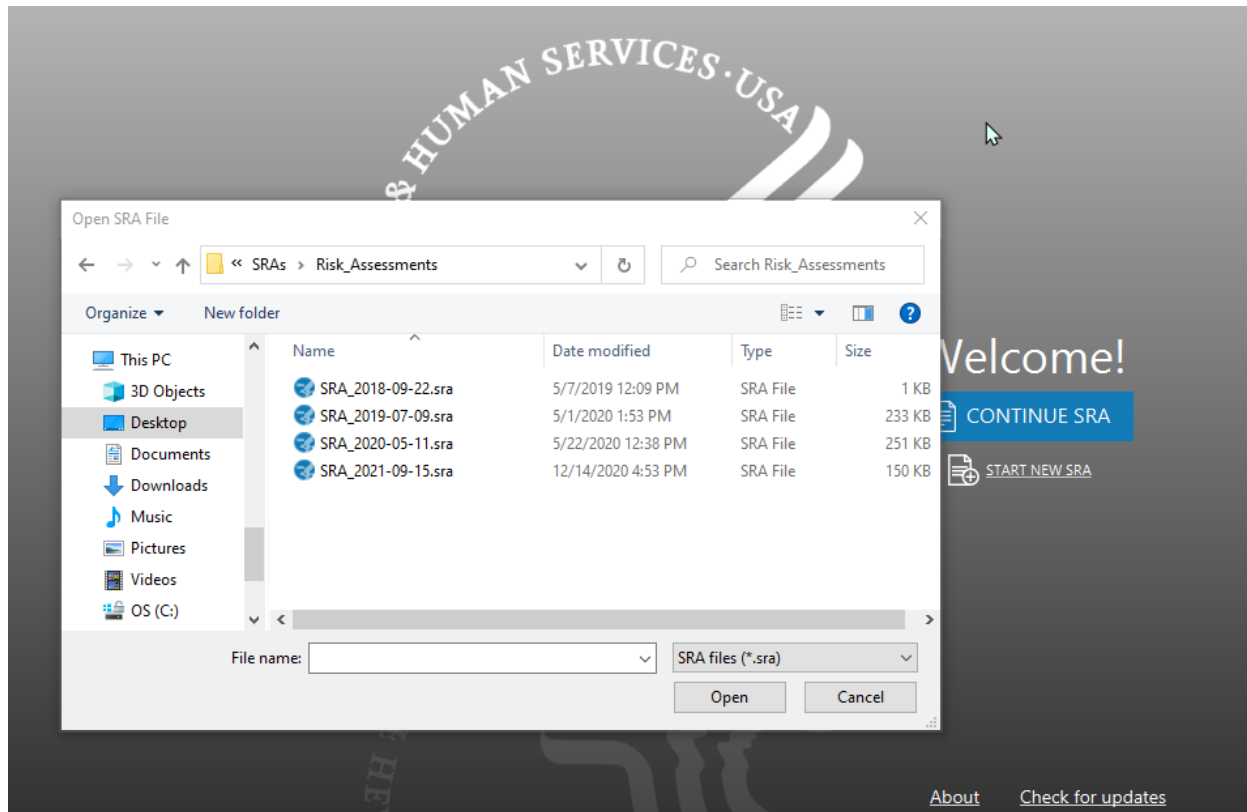
Starting a New Assessment



To start a new assessment, the SRA Tool must be downloaded and installed on a compatible Microsoft Windows operating system. The first steps to starting a new assessment are entering a username of your choosing, creating a file name for your SRA, and selecting a location to save your SRA file.

1. Select "START NEW SRA".
2. Enter a username. Click "Continue".
3. This can be simply a first name, first and last, initials, or anything else to distinguish the current user from any other parties intending to contribute to the risk assessment.
4. Select "Pick a spot to save your SRA file." This launches a system file browser.
5. To begin a new assessment and save progress, a location and file name for the SRA file must be selected. It is recommended to use a file name containing "SRA" and the current date so the file can be found more easily via search in the future, "SRA_9-3-2022.sra" for example.
6. Choose a location and file name for the assessment, click "Save" when finished. Click "Continue" to move forward.

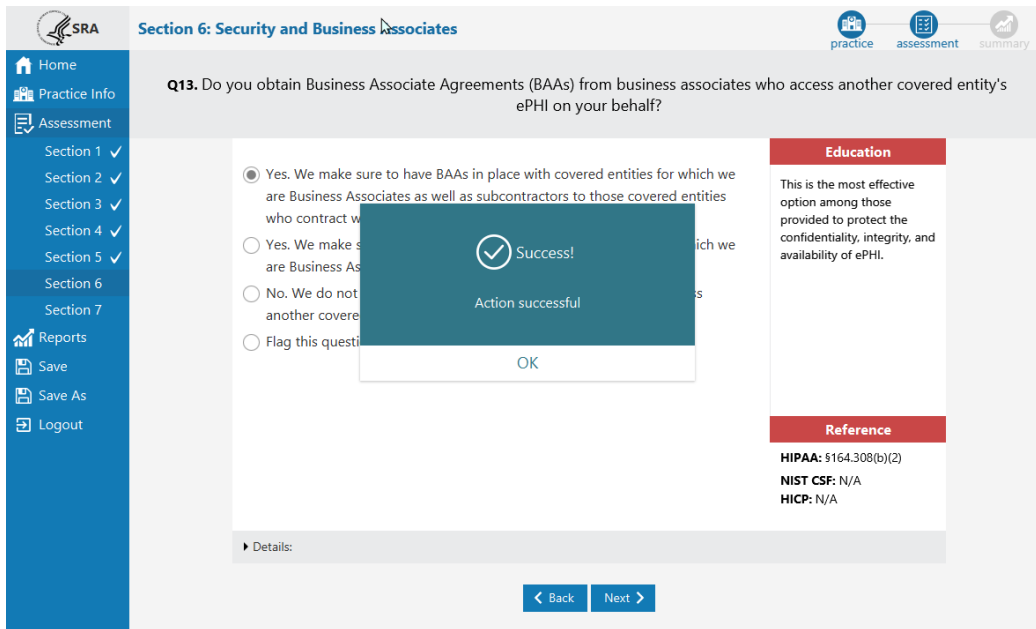
Continuing an Assessment



There are two ways to continue an old assessment or an assessment in progress:

1. Double-click file in Windows
 - a. On a computer with the SRA Tool installed, navigate to the location where an SRA file is saved.
Note: SRA Files can be identified by the blue SRA Tool icon and the "SRA File" file type, and the .sra extension (file extension may not be displayed depending on OS configuration).
 - b. Double-click the SRA file
 - c. The SRA Tool application will open the file in the state it was last saved
2. Open file using "Continue SRA"
 - a. Launch SRA Tool.
 - b. Select "Continue SRA"
 - c. Navigate to location with saved .sra file (note that you cannot open SRA tool 2.0 files with SRA 3.4 except for bulk uploads of asset and vendor information)
 - d. Select the previously saved assessment and click "Open"
 - e. Select existing user or create new user.
 - f. Continue assessment.

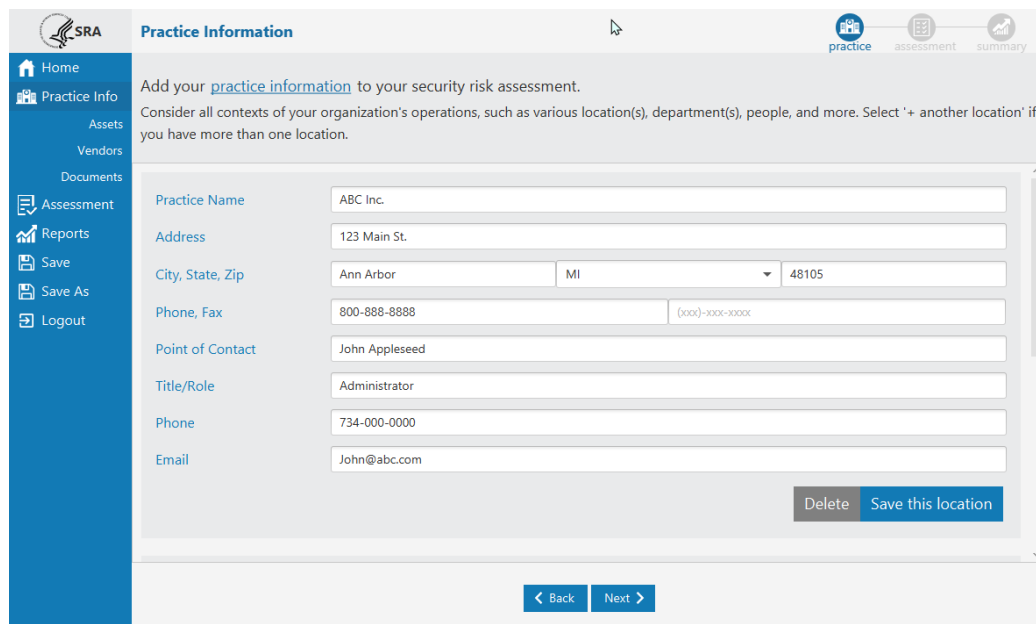
Saving Assessment Progress



Assessment progress can be saved at any time by clicking the Save button on the left navigation menu. Progress will be saved to the location the file was opened from. The tool will also ask you to save your assessment before exiting.

Save As allows the user to create another copy of their assessment under a different name or in a different location.

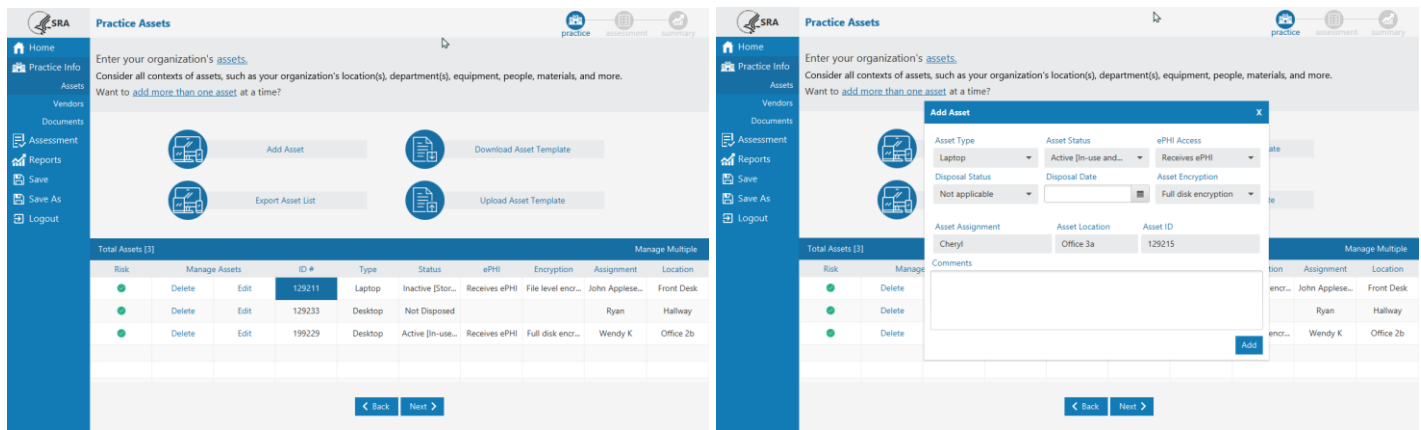
Add Practice Information



The SRA Tool provides a method to store practice information. Practice information is stored with assessment data and can be accessed by loading an SRA file and navigating to the Practice Info screen or by viewing the Detailed Report once the assessment is completed.

1. Enter information related to the practice. Select “Save this location” after each practice information section is completed.
2. Multiple practice locations can be added by clicking “add another location” After doing so, a new Practice Information section will appear. There is no limit on practices that can be added.
3. The “Delete” button can be used to remove any practice that is no longer needed. A prompt will appear directing the user to confirm the deletion of the selected practice.

Add/Edit Asset Information

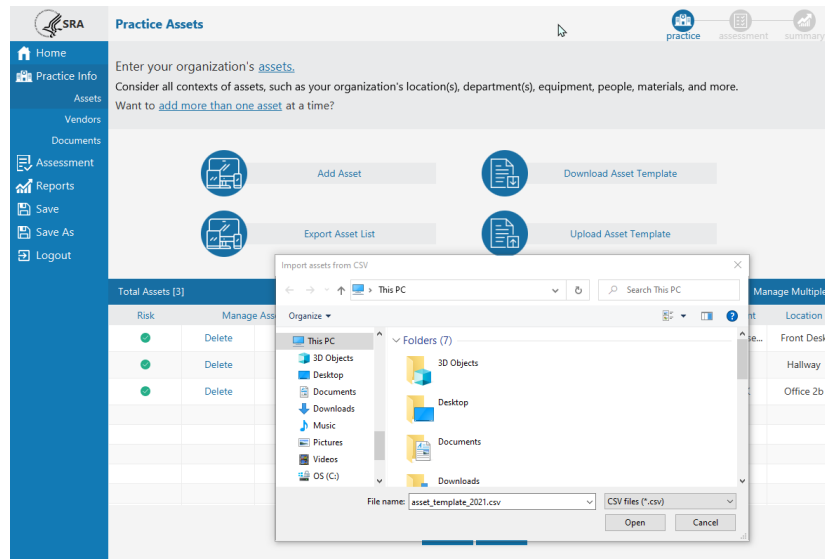


The SRA Tool provides a method to track IT assets at a practice(s). Assets are stored with the assessment data and can be accessed by loading SRA file in the SRA Tool and viewing the Practice Assets screen or by viewing the Detailed Report after an assessment has been completed.

1. Select the “**Add Asset**” button from the Practice Assets Page. This page can be navigated to by pressing “**Next**” after Practice Info or selecting “**Assets**” under the Practice Info item in the left navigation menu.
2. Enter information related to the asset:
 - a. **Asset Type**
 - b. **Asset Status** – is the asset currently in use?
 - c. **ePHI Access** – how does the asset interact with protected health information (PHI)
 - d. **Disposal Status** – If the device is no longer in use, was it disposed of?
 - e. **Disposal Date**
 - f. **Asset Encryption**
 - g. **Asset Assignment** – who, if anyone, is responsible for the asset?
 - h. **Asset Location** – where is the asset physically located?
 - i. **Asset ID** – any internal identification system used to uniquely identify the asset.
3. Select “**Add**” to add the asset. The asset will appear in the table at the bottom of the screen.
4. Selecting the “**X**” in the top right corner of the asset window will cancel the operation.
5. Previously entered asset information can be edited by selecting “**Edit**” next to an asset in the table at the bottom of the Practice Assets screen. The Edit Asset window will appear and behave similarly to the Add Asset window. Selecting “**Update**” at the bottom of the window saves changes.

- Assets can be deleted by selecting “Delete” next to a particular asset in the table in the bottom of the Practice Assets page.

Upload Asset Template (Bulk Operations)



	A	B	C	D	E	F	G	H	I
1	Type	Assignment	ID	Asset Status	ePHI	Encryption	Comment	Disposal Status	Disposal Date
2	Laptop	John Appleseed	CID-22120	Inactive [Storage]	Receives and transmits ePHI	Full disk encryption		Not Disposed	9/20/2018
3	Laptop		CID-22613	Active [In-use and Unassigned]	Receives ePHI	Full disk encryption		Not Disposed	9/20/2018
4	Desktop	Laura Jones	CID-22165	Active [In-use and Assigned]	Receives and transmits ePHI	Full disk encryption		Not Disposed	9/20/2018
5	Ultrasonography		CID-22145	Active [In-use and Unassigned]	Creates ePHI	File level encryption		Not Disposed	9/20/2018
6	Printer, Copier, Fax machine			Active [In-use and Assigned]	All of the above	No encryption		Not Disposed	9/20/2018
7									
8									
9									

Assets can be added and exported from the SRA tool in bulk. To do this, the tool uses a strictly formatted CSV template. Assets are exported from and imported to the tool following the template. A blank template file can be downloaded from the Practice Assets screen.

It is important to remember that in order to work with the SRA Tool, files must be kept in CSV format. **The tool does not accept .xls or .xlsx files. Ensure that files retain the .csv extension and file type.**

Once assets have been added to an SRA file using the SRA Tool, the entered assets can be exported to a CSV file.

- Select “Export Asset List” from the Practice Assets screen.
- Acknowledge the data security warning. It is important to remember that the exported asset list is stored in plain text, unencrypted. Do not leave this file where unauthorized personnel could gain access to it.
- Select a location and file name for the asset list. Select “Save”.

A blank asset template can be downloaded from the tool if a user wishes to import all assets from a CSV file.

- Select “Download Asset Template” from the Practice Assets screen.
- Select a location and file name for the asset template. Select “Save”.

Correctly formatted asset files can be uploaded to the tool as an alternative to manual entry from the user interface.

1. Add properly formatted asset information to a CSV file that follows the template.
2. Ensure that the file is saved as a .csv
3. Select the **“Upload Asset Template”** button from the Practice Assets screen
4. Navigate to and select the saved CSV file. Select **“Open”**.
5. Imported assets will appear in the table at the bottom of the Practice Assets screen.

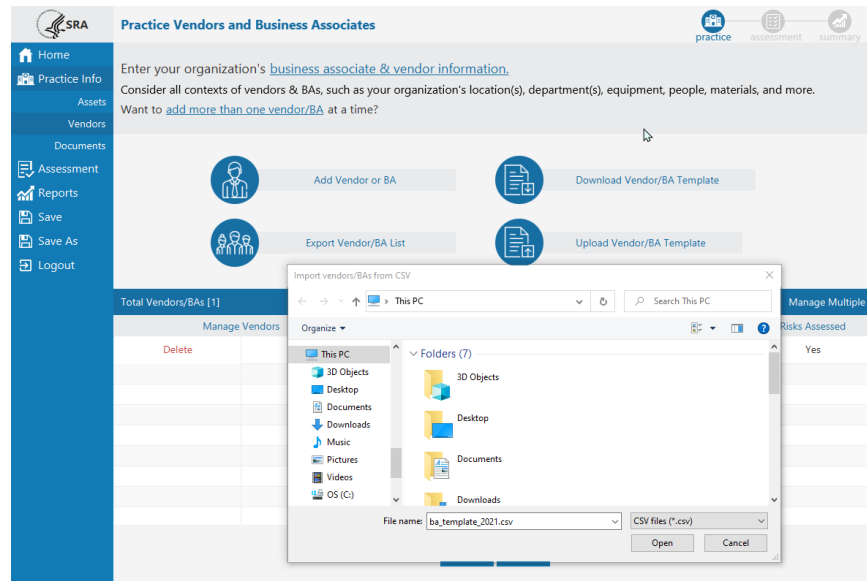
Add/Edit Vendor Information

The SRA Tool Provides a method to track Vendors or business associates. Vendor information stored with the assessment data and can be accessed by loading SRA file in the SRA Tool and viewing the Practice Vendors screen or by viewing the Detailed Report after an assessment has been completed.

1. Select the **“Add Vendor or BA”** button from the Practice Vendors Page. This page can be navigated to by pressing **“Next”** after Practice Assets or selecting **“Vendors”** under the Practice Info item in the left navigation menu.
2. Enter information related to the Vendor:
 - a. **Vendor Name**
 - b. **Service Type Provided**
 - c. **Vendor Address**
 - d. **Phone, Fax**
 - e. **Contact Name/Title** – primary contact from vendor
 - i. **+Second Contact** – a second contact can be recorded for a particular vendor. Selecting the **“+Second Contact”** button loads two additional contact fields for title and email. Clicking the button again will collapse the additional fields.
 - f. **Contact Email**
 - g. **Satisfactory Assurances** – written agreement to safeguard protected health information.
 - h. **Risks Assessed**

3. Select “**Add**” to add the vendor. The vendor will appear in the table at the bottom of the screen.
4. Selecting the “**X**” in the top right corner of the add vendor window will cancel the operation.
5. Previously entered asset information can be edited by selecting “**Edit**” next to a vendor in the table at the bottom of the Practice Vendors screen. The Edit Vendor window will appear and behave similarly to the Add Vendor window. Selecting “**Update**” at the bottom of the window saves changes.
6. Vendors can be deleted by selecting “**Delete**” next to a particular vendor in the table in the bottom of the Practice Vendors page.

Upload Vendor Template (Bulk Operations)



	A	B	C	D	E	F	G	H	I	J
1	Vendor Name	Service Type	Address	City	State	Zipcode	Phone	Fax	Contact N	Contact
2	Lab Testing llc.	laboratory services	111 Hoover Ave.	Ann Arbor	MI	48103	734-555-2222			
3	Cleaners	cleaning service	1909 Washtenaw Ave	Ann Arbor						
4										
5										
6										
7										
8										
9										

Vendor information can be added and exported from the SRA tool in bulk. To do this, the tool uses a strictly formatted CSV template. Vendors are exported from and imported to the tool following the template. A blank template file can be downloaded from the Practice Vendors screen.

It is important to remember that in order to work with the SRA Tool, files must be kept in CSV format. **The tool does not accept .xls or .xlsx files. Ensure that files retain the .csv extension and file type.**

Once vendors have been added to an SRA file using the SRA Tool, the entered vendors can be exported to a CSV file.

1. Select “**Export Vendor List**” from the Practice Vendors screen.

2. Acknowledge the data security warning. It is important to remember that the exported vendor list is stored in plain text, unencrypted. Do not leave this file where unauthorized personnel could gain access to it.
3. Select a location and file name for the asset list. Select **“Save”**.

A blank vendor template can be downloaded from the tool if a user wishes to import all vendors from a CSV file.

1. Select **“Download Vendor Template”** from the Practice Vendors screen.
2. Select a location and file name for the vendor template. Select **“Save”**.

Correctly formatted vendor files can be uploaded to the tool as an alternative to manual entry from the user interface.

Link Additional Documentation

The Documentation section allows users to link to supporting or supplemental documentation to the assessment.

No documents will be imported into and saved into the SRA tool, the tool allows users to save links to documents stored locally or on a local network to demonstrate accuracy and thoroughness of your responses and assessment.

Manage Documents	Document Name	Section	Added By	Date Added
Delete	template_QA4.csv	N/A	Ryan	03-15-2022
Delete	detailed_pdf_QA5.pdf	N/A	Ryan	03-15-2022

For example, vulnerability scans, penetration test results, plan of action milestones document, or mitigation plan are all documents that can be linked to your SRA file in this section of the tool.

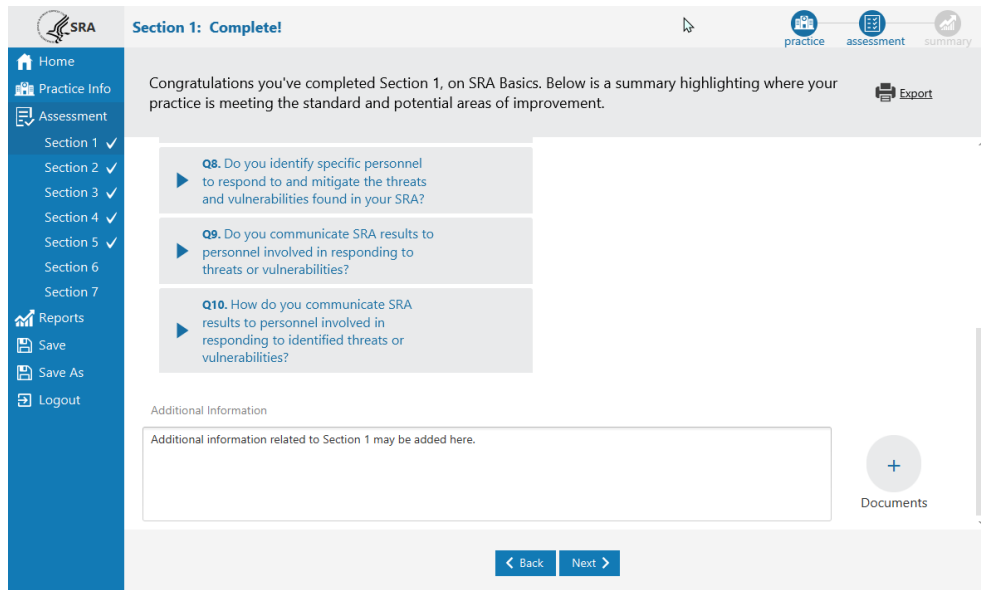
To link supplemental documentation to your SRA:

1. Click **“Add a Document”**
2. Within the Window File Library, navigate to the location where the document is saved.
3. Select the document you want linked to the assessment and click **“Open”**.
4. The file name and the link extension to the documentation will appear in the table below.

Note: This table also collects and lists documents that have been added to the assessment from the section summary.

Users can also link documentation specific to an assessment section. On each section summary screen, a comments box and **“Documents”** button are available.

SRA Tool v3.4 User Guide

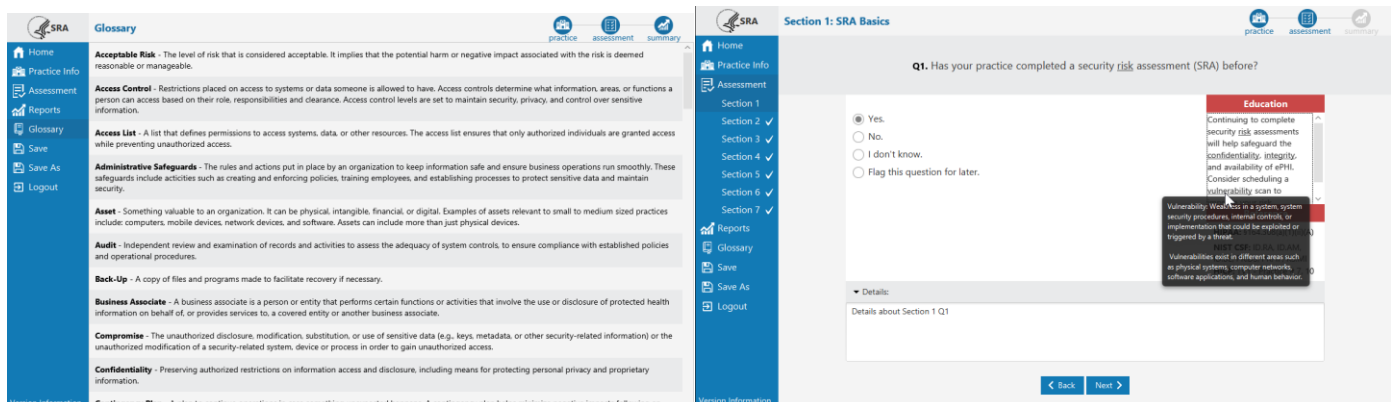


Users can note specific comments related to the section in the “Additional Information” comments box or link additional documentation by following these steps.

1. Click “**Documents**” button.
2. Within the Window File Library, navigate to the location where the document is saved.
3. Select the document you want linked to the assessment and click “Open”.
4. The file name and the link extension to the documentation will appear in the table below and in the documents table within the Documents section of the tool.

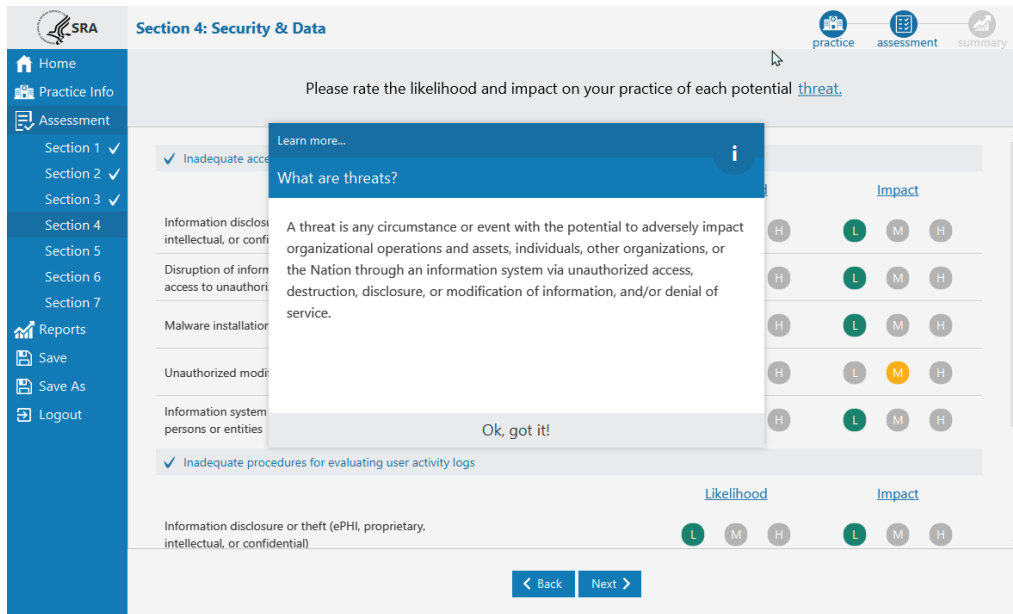
Glossary Terms

A glossary page is provided in the left navigation menu for reference. This glossary of terms may be updated over time through subsequent SRA Tool releases. The glossary is provided as a static page, but also as contextual tooltips which are displayed when a user hovers over a highlighted term. Glossary terms in the content can be identified by an underline in the question and education text.

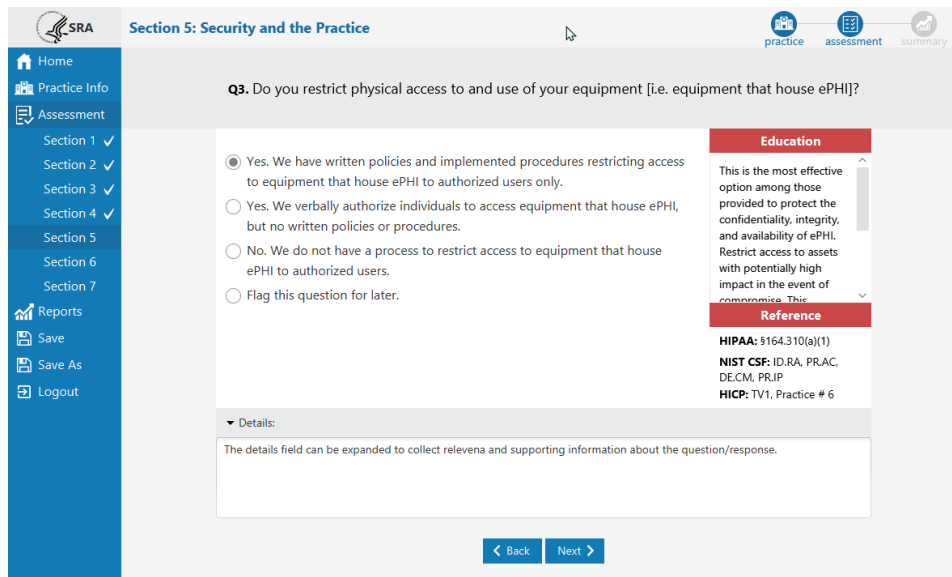


SRA Tool v3.4 User Guide

Some terms throughout the tool are identified as hyperlinks with blue underlined text. Clicking on these terms launches a popup window that may provide richer information underlined glossary terms as shown on the previous page. These popups may contain hyperlinks to external content, for example.



Completing the Assessment



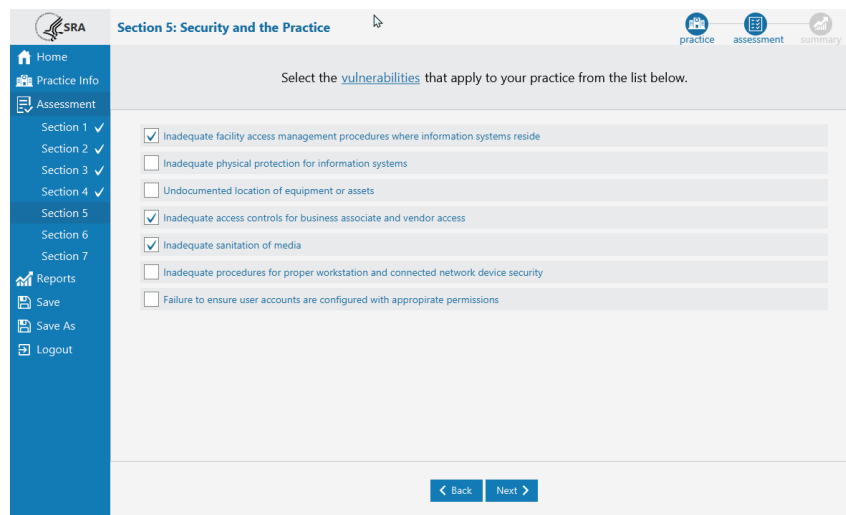
The assessment portion of the tool is broken down into sections. A list of sections can be seen on the left side of the screen while completing the assessment. The assessment contains branching logic that may serve questions in a different order depending on different response selections.

1. Each question in the assessment portion is single answer and multiple choice. This means that one answer and only one answer must be answered to continue.
2. The question number is displayed to the left of the question text. Questions are numbered starting at

“Q1” for each section.

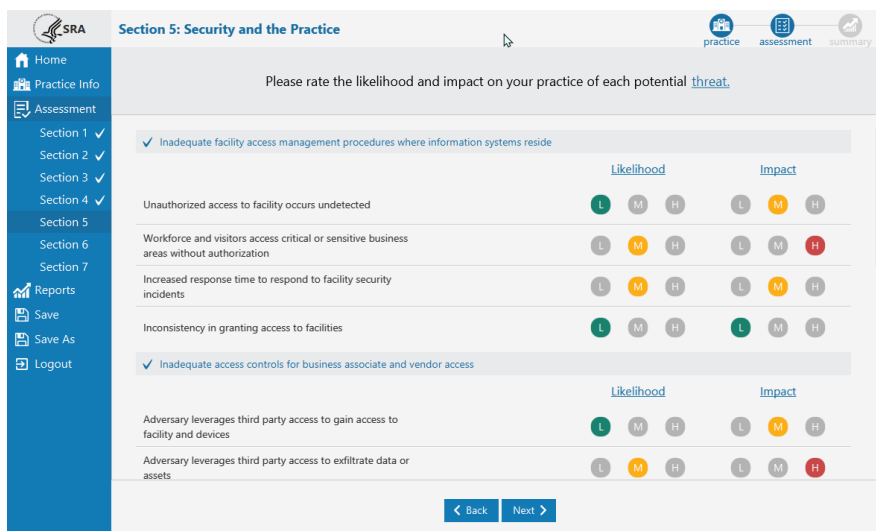
3. The **Education** panel on the right side of the screen. When no answer is selected, the panel will be blank. Once a selection is made, information relevant to that selection will be displayed in the panel.
4. The **Reference** panel is on the right side of the screen. Reference to relevant security information regarding the question is shown here. References can be selected to get more information about the related documents. Links to HHS and NIST web resources are provided.
5. The **Details** box can be used to capture supporting information or notes about an individual question. This free text field can be expanded and collapsed by clicking on the “Details” label.
6. Selecting “**Next**” at the bottom of the screen progresses to the next question or section. After each multiple-choice section, a threats and vulnerabilities rating section will be presented.

Threat & Vulnerability Rating



After completing each section of multiple-choice questions, a set of vulnerabilities is presented. Multiple items can be selected. Select each vulnerability applicable to your practice.

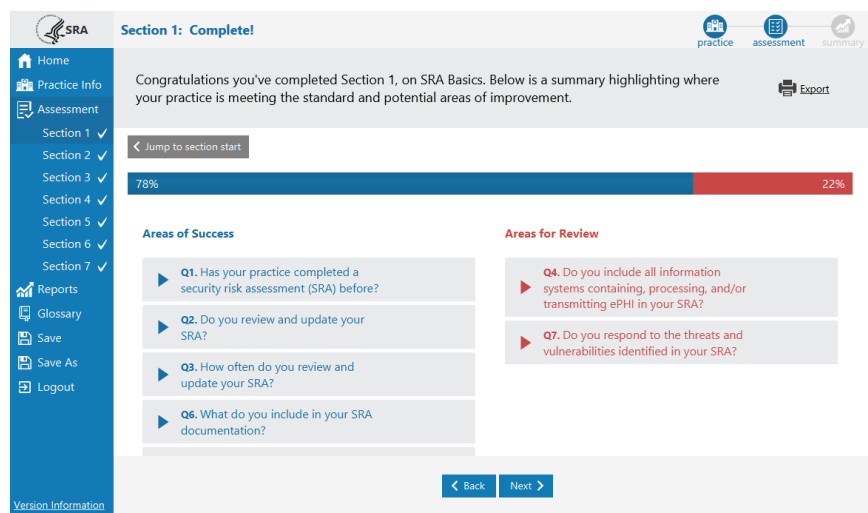
1. Check the check box next to each applicable vulnerability.
2. Select “**Next**” to continue.



Each selected vulnerability has associated threats. Each threat must be rated based on the likelihood of occurrence at a practice, and the impact it would cause.

1. Make a selection for “**Likelihood**” and “**Impact**” for each threat listed.
 - a. L = Low
 - b. M = Medium
 - c. H = High
2. Both likelihood and impact for each threat must be rated before users can continue to the next screen.
3. Select “**Next**” to continue.

Section Summary



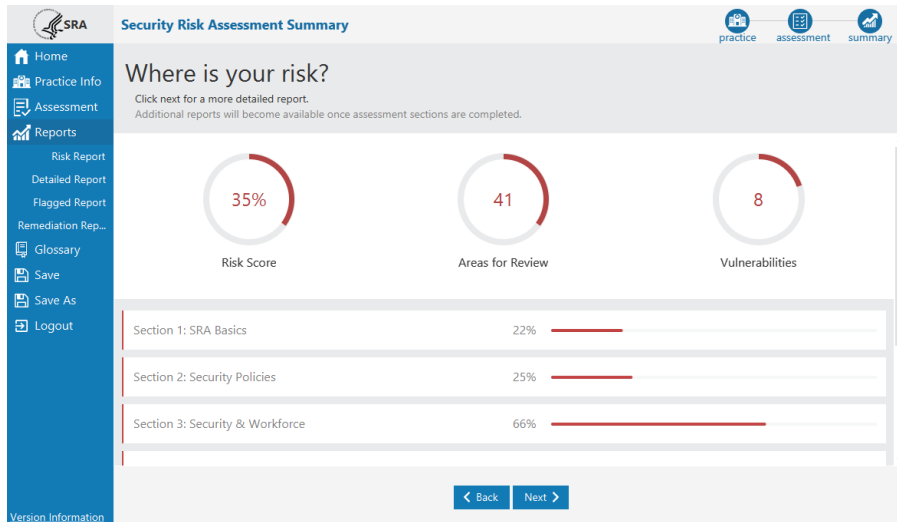
After completing multiple choice, threat selection, and vulnerability rating, a section summary is presented.

1. **Areas of Success** presents a list of questions where responses met the expectation, indicating compliance.
2. **Areas for Review** lists questions where responses indicated expectations are not being met, and review of process and procedures may be needed to improve safeguard efforts.
3. Clicking on the triangle on the left side of each question expands a tile revealing the chosen response and education information.
4. The graphic at the top of the screen represents the percentage of responses in the Areas of Success and Areas for Review categories respectively.
5. The **Export** button near the top right corner of the screen can be used to export a PDF copy of a section summary.
6. The **Jump to section start** button near the top left corner of the screen serves as a navigational shortcut. It provides an easy way to move back to the beginning of the section. All question responses from a completed section are preserved when using this feature.

Note: When you move back to the beginning of a section, you must progress to the end again for the section to register as complete. Section completion is signified by a white check mark next to the

section number in the navigation menu.

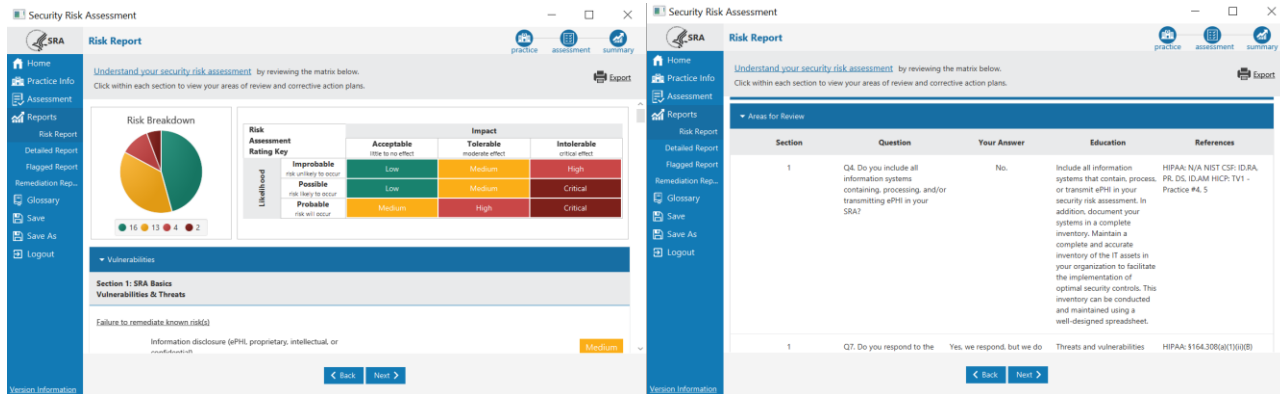
Assessment Summary



When all assessment sections have been completed, the SRA Summary screen is displayed. This screen shows percentages and visual representations of scores across all sections of the assessment.

1. **Risk Score** – percentage of responses sorted into Areas for Review across the whole assessment.
2. **Areas for Review** – count of responses sorted into the Areas for Review category.
3. **Vulnerabilities** – count of vulnerabilities selected as applicable to the practice.
4. **Section risk scores** – a percentage of responses sorted into Areas for Review for each section.

Risk Report



The Risk Report highlights responses from the multiple choice, threat, and vulnerability sections that indicate risk.

1. **Risk Breakdown** – This pie chart shows the proportion of threats in each rating category. The key below gives counts of threats in each category.
2. **Risk Assessment Rating Key** – This key shows how overall risk rating is calculated by combining threat likelihood with threat impact.
3. **Vulnerabilities** – All selected vulnerabilities are listed here along with their associated threats. Vulnerabilities are grouped by section
4. **Areas for Review** – All questions and responses sorted into Areas for Review are listed here along with education. Questions are grouped by section.
5. Both Vulnerabilities and Areas for Review can be collapsed by clicking on the white triangle to the right of the respective headings.
6. The **Export Options** button in the top right corner of the screen allows the report to be exported as a PDF.

Detailed Report

Click each section to expand and review more details.

Disruption of business processes or information system function	Medium
Social engineering attack or email phishing attack	Low
Misuse of information systems and/or hardware	Low
Information system or facility access granted to unauthorized personnel	Low
Installation of unauthorized software or applications	Critical

Question	Answer	Education	References	Compliance Guidance/Rule	Username	Date/Time
Q1. Who within your practice is responsible for developing and implementing information security policies and	The role of security officer is described in our policy documentation, but the person who occupies that role is not named.	You should have a qualified and capable person appointed to the responsibility of security officer. Having a central point of contact	HIPAA: §164.308(a)(2) NIST CSF: PR.AT, DE.DP, ID.IGV RS.CO, PR.IP, ID.AM HICP: TV1 - Practice # 10	Required	Dawn 3.4 test	Wed Aug 16 14:24:46 EDT 2023

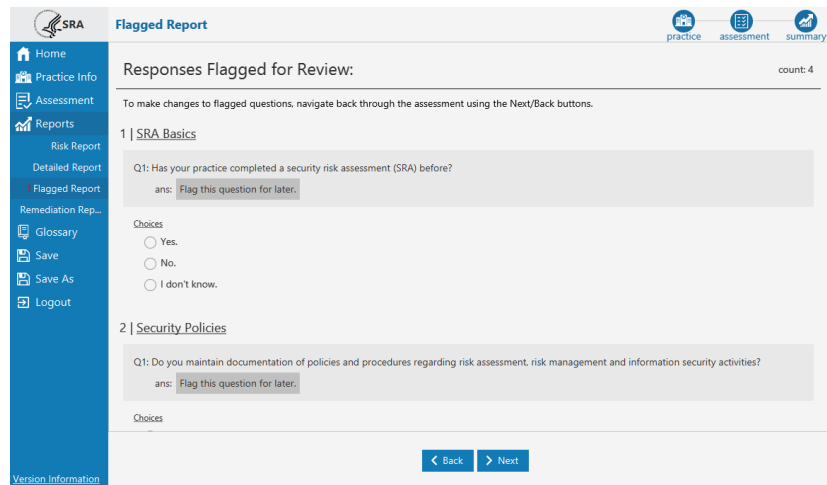
Version Information

< Back Next >

The Detailed Report is an output of all the information entered into the SRA Tool, besides section comments and linked files. Each section is broken down into threats & vulnerabilities and multiple choice.

1. Each section is collapsible. Select the section title or black triangle to expand a section. Click again to collapse.
2. **Risk Score**, that is the percentage of multiple-choice responses sorted into Areas for Review, is displayed for each section.
3. **Risk Rating** is a combination of likelihood and impact rating for each threat. The Risk Assessment Rating Key on the Risk Report shows how Risk Rating is calculated.
4. Practice Information, Asset Information, and Business Associates and Vendors are all displayed at the bottom of the Detailed Report.
5. The **Export Options** button at the top right corner of the report allows the Detailed Report to be saved as a PDF. Click the icon and select a name and location to save the PDF file.

Flagged Report



The Flagged Report is a list of all questions marked with “Flag this question for later.” It displays the section, question number, question text, list of responses, and the chosen response.

This report is not interactive. To make changes to responses shown in the risk report, you need to navigate back through the assessment. To do this, click on the “Assessment” menu item. Click “Next” until you reach the section summary for the question you wish to change. From the section summary, click “Back” until you reach the question and response you would like to change. Upon changing your response, click “Next” to view the next sequence of questions (a change in response may lead to new previously unanswered questions).

Remediation Report

Like the Risk Report, the Remediation Report presents all questions where risk was indicated. These are all questions sorted into “Areas for Review” at the end of each section.

The Remediation Report provides a place for responses to risk to be recorded. For example, if risk is indicated because the practice does not review access to systems containing ePHI, plans for reviewing this access can be detailed under “Remediation Activities.”

This section is optional to complete within the tool. Areas of risk always require response, but these response plans may be documented outside the SRA Tool.

To use this report, simply click on it from the left navigation panel and select “Add Remediation” and begin to enter Remediation Activities. Remember to click “Save Remediation” so responses are saved to your file.

1. **Sections Selector** – The Sections Selector at the top of the page controls navigation between sections of the tool. There is a page for each section in the report and they must be navigated to using the Sections Selector.
2. **Remediation Activities** – Text area to be used for documenting response to risk identified for each question in the report.
3. **Owner** – Text field to assign an owner for the remediation activity. This is a way of indicating responsibility for improving response to risk.
4. **Due Date** – Date field that may be used to track deadlines to respond to risk.
5. **Date Completed** – Date field used to track when a remediation activity is completed.
6. **+ Link Documentation** – Allows linkage to documentation on a local or network drive.
7. **Save Remediation** – This must be clicked for changes to be saved to the .sra file. After clicking this button, the remediation action will change to a read-only state. It can be reopened for editing by selecting “Edit Remediation”.

Saving & Exporting

There are a few ways to save information in the SRA Tool:

1. Save Detailed Report as PDF or Excel

The Detailed Report is a complete output of information captured by the tool minus section comments and linked documents. It contains Practice Information, Assets, Vendors, multiple choice, vulnerabilities, and threats.

The Detailed Report can be saved as a PDF or Excel by clicking the “**Export Options**” link near the top right corner of the report screen.

2. Export Asset List

Asset information from the tool can be exported as a CSV file by selecting “**Export Asset List**” from the Asset Information screen. This is a useful method to move assets from one SRA file to another without re-entering each one individually.

3. Export Vendor List

Vendor information from the tool can be exported as a CSV file by selecting “**Export Vendor List**” from the Vendor Information screen. This is a useful method to move vendor information from one SRA file to another without re-entering each one individually.

Version Information

There are two types of versioning that must be considered with the SRA Tool: SRA Tool Version and Content Version.

The screenshot shows the SRA Tool interface. On the left is a blue navigation menu with items: Home, Practice Info, Assessment, Reports, Glossary, Save, Save As, and Logout. The main content area has a 'Welcome!' header and a 'What is a Security Risk Assessment?' section. A 'Version Information' dialog box is open in the center, displaying:

Current Application Version
SRA Tool: 3.4
Current Content Version
Content Set: 3.4

Below the dialog, the 'The SRA Tool' section lists three steps: Step 1: Enter your practice information. Step 2: Answer the assessment questions. Step 3: Review your final risk report. A 'Next >' button is at the bottom right.

SRA Tool Version

The SRA Tool version is the version of the SRA Tool software you are using. This corresponds with the installer downloaded from HealthIT.gov. The installer will always contain version in the file name so you know which version of the tool you are installing.

To confirm which SRA Tool version you are using, you may look in the following places:

1. **Check for updates** link on the SRA Tool Welcome Screen. Located in the bottom, right corner of the screen before login.
2. **Version Information** located in the bottom, left corner of each screen inside the tool once logged in. Two versions may be shown here, “Current Application Version” shows the SRA Tool version.

CONTENT VERSION

Content version refers to the questions, education, references, and glossary information provided in the tool. Content version may be different from SRA Tool version. For example, you may open an assessment (SRA File) created with version 3.2 of the SRA Tool. This file was created with questions available at the time and is not upgraded when opened with a later version of the tool.

CONTENT VERSION OUT-OF-DATE WARNING

Upon logging into the SRA Tool with a pre-existing SRA File, an informational warning may appear. This means that the file you are working on is not in sync with the latest version of the SRA Tool application. You may continue to use the file, but you will not be able to take advantage of updates to questions and content unless you start a new file. This warning cannot be dismissed, it will appear each time the file is opened.

The warning may read “Content in this file: N/A”, this means that the file contains questions or content that are version 3.3 or older.

SRA Tool Excel Workbook

The SRA Tool Excel Workbook contains the same multiple-choice questions, education, references, and risk score system that is found in the SRA Tool desktop application.

The Excel workbook can be downloaded on the SRA Tool download page on HealthIT.gov alongside the SRA Tool desktop application and this user guide.

Section 1 - SRA Basics							
Question #	Question Text	Response Indicator	Question Responses	Guidance	Risk Indicated	Required?	Reference
1	Has your practice completed a security risk assessment (SRA) before?		Yes.	Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 7, 10
		<input checked="" type="checkbox"/>	No.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.	Review	Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 7, 10
			I don't know.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 7, 10
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 7, 10
	Notes						
2	Do you review and update your SRA?		Yes.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 10
			No.	Consider reviewing and updating your security risk assessment periodically. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 10
			I don't know.	Consider reviewing and updating your security risk assessment periodically. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 10
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: TVL, Practice # 10
	Notes						
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE RS.MI HICP: N/A
	Notes						
Threats & Vulnerabilities							
					Likelihood	Impact	Risk Score
1	Inadequate risk awareness or failure to identify new weaknesses		Non-physical threats(s) such as data corruption or Physical threats such as uncontrolled facility access. Natural threat(s) such as damage from fire/particulates, Man-Made threat(s) such as insider carelessness, Intelligence threats(s) such as leaking/overhearing.		Low High Medium Medium	High Medium High Low	High High Critical Low
2	Failure to remediate known risks		Information disclosure (ePHI, proprietary, intellectual, or penalties from contractual non-compliance with third- Disruption of business processes, information systems Data deletion or corruption of records Prolonged exposure to hacker, computer criminal, Corrective enforcement from regulatory agencies (e.g. Hardware/equipment malfunction		Medium Low Medium Low	Medium Medium Low High	Medium Medium Low High
3	Failure to meet minimum regulatory requirements and security standards		Corrective enforcement from regulatory agencies (e.g. Damage to public reputation due to breach Failure to train incentives or enforce value-based Litigation from breach victims due to lack of reasonable		High High Medium High	Low High High High	Medium High Critical High
4	Inadequate AUP tracking		Information disclosure (ePHI, proprietary, intellectual, or Disruption of business processes, information systems Unauthorized use of assets or changes to data within Unauthorized installation of software or capabilities Loss, theft, or disruption of assets Improper operation/configuration of assets		Medium Low Medium Low	Medium Low Low High	Medium Medium Low High
5	Unspecified workforce security responsibilities		Non-remediated weaknesses Prolonged duration of addressing non-remediated Insider carelessness regarding email or causing disruption		High High Medium High	High High High High	High High High High

1. Sheets for all seven SRA Tool sections are included. Each sheet should be reviewed to complete a risk assessment.
2. Select question responses using the drop-down in the **Response Indicator** column in the row that corresponds to the desired response. Responses are marked using the “✓” symbol.
3. Responses indicating areas for review will automatically be highlighted in yellow.
4. The Threats & Vulnerabilities section at the bottom of each sheet contains a list of vulnerabilities related to that section and their associated threats.
5. Rate threats for vulnerabilities that are applicable to your organization. Rate threats based on the **Likelihood** of a threat occurring and the **Impact** it would have on your organization should it occur.
6. The **Risk Score** is automatically assigned based on the matrix in the Risk Logic sheet. This is the same score that is assigned in the SRA Tool desktop application.

Frequently Asked Questions [FAQ's]

Is the SRA Tool compatible with MacOS?

No, the SRA tool is only compatible with Windows. The SRA Tool Excel Workbook, available on HealthIT.gov, may be a reasonable alternative for those unable to install the SRA Tool.

How do I print my results (save as PDF or Excel)?

Once all sections of the assessment are completed, reports become available. The Detailed Report provides the most complete output of your assessment. "Export Options" near the top right corner of the screen will launch a Save As dialog and allow saving the assessment information as a PDF or Excel. Section Summaries can also be exported to PDF as sections are completed.

Is it possible to get printable sheets for each section of the SRA?

The best way to do this is to download the SRA Tool Excel Workbook. These can be printed.

How do I access the Summary Reports?

To access reports available under the Summary menu item, the assessment must first be 100% completed. Once a section is completed, a white check mark will appear to the left in the navigation menu. When all sections have check marks, the Summary menu item will become available.

Does the tool keep record of date completed?

The Detailed Report shows a date and timestamp next to each question answered. This date reflects the date a response was last modified. This timestamp will not update unless the response is changed.

Is it possible to add new assessments each year without risking overwriting last year's assessment?

With each new assessment, the user is asked to select a file name and save location for the .sra file. As long as the previous year's file is not selected and overwritten, this should not be an issue. If you wish to make amendments to a previous year's assessment versus starting from scratch, you may consider loading a previous year's assessment and using the "Save As" feature to rename the file to reflect a new year's SRA.

Is there an easy way to show the risk assessment has been reviewed even if nothing changed? If so, how?

If you wish to make amendments to a previous year's assessment versus starting from scratch, you may consider loading a previous year's assessment and using the "Save As" feature to rename the file to reflect a new year's SRA. The timestamp for individual questions will remain the same, questions are marked with the date they were last modified. All questions throughout the tool should be reviewed even if their responses will remain unchanged.

How do I go back and edit my assessment?

The SRA Tool uses branching logic to serve questions most relevant to your practice. This limits your ability to select a specific section and or question to edit.

To edit a response, first click the "Assessment" item in the left navigation menu. Click "Next" to proceed through each section. If a section has been completed, you will only see its section summary. Once you have navigated to the desired section, select the "Back" button to move backwards through each question until you

reach the item you wish to edit.

Keep in mind that changing a response may set you on a different course in the branching logic, requiring you to answer a different set of questions to complete the section.

Is there an updated version of the paper version of the SRA?

Yes, the SRA Tool Excel workbook is provided for download on the HealthIT.gov download page. The Excel workbook contains the same questions, guidance, and references as the desktop application. It is an interactive spreadsheet that highlights areas indicating risk and indicates risk score for threats and vulnerabilities.

Will there be support for the TEFCA rule in the SRA per Section 6.2.1 of January 2018 draft of TEFCAs? The TEFCAs reference the NIST 800-53 and the CUI. At some point an SRA for the QHINs will be needed. Will this be added?

TEFCA support may be considered for a future version after the TEFCAs rule is finalized.

Will video help be added to Version 3.4?

A video recording of the SRA Tool webinar is available on HealthIT.gov.

<https://www.youtube.com/watch?v=w4b-74rTRbo>

Is there support for penetration testing in Version 3.x?

Results from independent penetration testing can be uploaded into the tool. However, the tool does not include penetration testing capabilities, nor does it provide guidance on how to conduct penetration testing. The primary focus of the SRA Tool is to aid in the Security Risk Assessment process. Results from external penetration tests or vulnerability scans can be added to the tool as supporting documentation regarding an entity's overall security risk assessment process.

Will a future version of the security risk assessment tool be developed for patients so they can better understand the risks they are agreeing to by using healthcare apps?

There's coordination between the FTC and the HIPAA security rule. NIST has been leading a privacy consumer base with the Department of Commerce and are working on an initiative to inform consumers about their risk. For general information about whether mobile apps are covered by HIPAA, visit <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>

Is the SRA tool suitable for large practices or covered entities?

The SRA Tool was designed with small to medium sized practices in mind, but the content is still applicable to practices of all sizes. That said, large organizations may find other methods more suitable to conducting an SRA.

If a practice has multiple locations, can one SRA be completed to cover all of them, or should multiple SRAs be conducted?

The answer to this depends on how much the locations differ with their policies, procedures, and infrastructure. If you feel that the questions being answered are applicable to all locations, one SRA may be sufficient. If question responses are not applicable to all locations, you may consider doing a separate SRA for each location.

If you already have an excel file with assets created by our 3rd party, can that be uploaded?

Lists of assets can be linked to your SRA using the Documents feature. This feature allows you to link documents located on your local machine or another networked location.

Do we need to list every device on our network as an asset?

Keeping an inventory of assets that have access to ePHI is an important part of assessing your security posture. Even assets that do not have access to ePHI can open your IT environment up to compromise. See this OCR newsletter on keeping an asset inventory for more information <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2020/index.html>

How is the Risk Rating determined?

Risk Rating is determined based on the Risk Assessment Rating Key shown at the top of the Risk Report. A threat rated with low likelihood and low impact will be assigned a Risk Rating of “low”.

How is the Risk Score percentage determined?

Risk Score is a percentage of responses marked as “Areas for Review” out of the total number of questions answered. In other words, it is the percentage of responses where risk was indicated.

Can SRA files be saved on shared network storage or in the cloud?

Yes. SRA files can be stored on a shared resource, whether it be on the cloud or otherwise. The file can be opened and saved in that location. This makes it easier for different users working on the same .sra file.

Does the SRA need to be submitted?

The SRA does not need to be submitted. Documentation supporting that an accurate and thorough risk analysis was conducted is required by HIPAA and should be kept on record.

Is any information from the tool sent to ONC?

All information captured by the tool stays with the .sra file. This is a local application that does not store any information on the internet. No information is sent to ONC.

How do I go back, and correct items listed in the Flagged Report?

To make changes to responses shown in the risk report, you need to navigate back through the assessment. To do this, select the section containing the question you would like to change. This will take you to the Section Summary screen. From here, you can either use the Back button to move backwards until you reach the desired question, or you can use the “Jump to section start” button to move to the beginning of the section and navigate forwards using the Next button.

When you’ve moved backwards from the Section Summary of a completed section, the white check mark signifying section completion will go away. In order to register as complete, you must navigate to the end of a section when finished editing. The white check mark will appear confirming section completion.

Where can I stay up to date with the latest SRA Tool developments?

Follow along with updates from ONC at HealthIT.gov and subscribe to the OCR Listserv.

OCR Listserv - <https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html>

ONC Email Updates – use “stay connected with ONC” on bottom of the page at [HealthIT.gov](https://www.healthit.gov)