



# Security Risk Assessment Tool v3.6

## 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](http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html)

NOTE: The NIST, HICP, and HPH CPG 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: August 7, 2025

## Contents

---

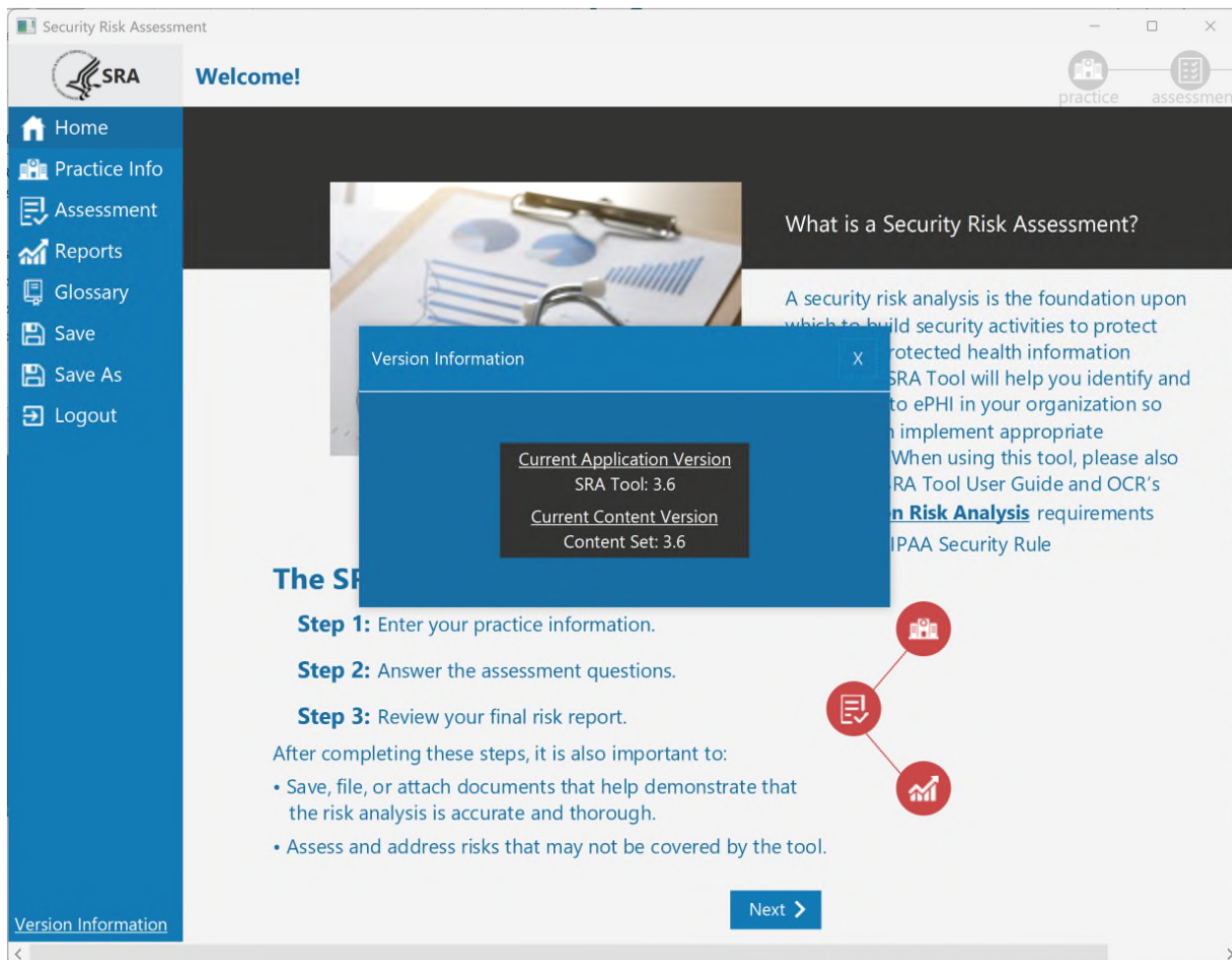
|   |    |
|---|----|
| WHAT'S NEW IN VERSION 3.6.....                | 3  |
| BACKGROUND .....                              | 4  |
| SRA Tool Overview .....                       | 4  |
| What to expect with the SRA Tool .....        | 4  |
| End User Hardware Requirements.....           | 6  |
| Download Instructions .....                   | 7  |
| USING THE TOOL.....                           | 8  |
| Starting a New Assessment.....                | 8  |
| Continuing an Assessment .....                | 10 |
| Saving Assessment Progress .....              | 11 |
| Add Practice Information .....                | 12 |
| Add/Edit Asset Information .....              | 12 |
| Upload Asset Template (Bulk Operations).....  | 13 |
| Add/Edit Vendor Information .....             | 14 |
| Upload Vendor Template (Bulk Operations)..... | 15 |
| Link Additional Documentation .....           | 16 |
| Glossary Terms .....                          | 17 |
| Completing an Assessment .....                | 18 |
| Threat & Vulnerability Rating.....            | 18 |
| Section Complete Summary.....                 | 20 |
| Security Risk Assessment Summary.....         | 21 |
| Risk Report .....                             | 21 |
| Detailed Report .....                         | 22 |
| Flagged Report .....                          | 23 |
| Remediation Report .....                      | 23 |
| Saving & Exporting .....                      | 25 |
| Version Information .....                     | 25 |
| SRA Tool Application Version .....            | 25 |
| SRA Tool Content Version.....                 | 26 |
| Content Version Out-of-Date warning .....     | 26 |
| SRA TOOL EXCEL WORKBOOK.....                  | 27 |
| FREQUENTLY ASKED QUESTIONS (FAQS).....        | 28 |

## What's new in version 3.6

The Security Risk Assessment (SRA) Tool version 3.6 includes enhancements and improvements based on current cybersecurity guidance and user feedback from previous versions.

New features and updates in SRA Tool Version 3.6 include:

- ▲ **A new assessment confirmation button with a “reviewed-by” date for each section.** This allows users to confirm a section has been reviewed and approved, with the approver's username and date of approval saved for audit records.
- ▲ **Updated risk scale to match NIST scoring.** The score of "medium" has been changed to "moderate" within the application, reports, and the Workbook version.
- ▲ **Updated reports with new content.** Report covers include updated disclaimers and the Detailed Report PDF now includes section-specific approval/reviewed-by details and additional information entered by users.
- ▲ **Updated library files that are included when users install the application.** This is important in mitigating potential vulnerabilities in outdated files.
- ▲ **Content improvements in questions, responses, and education.** These changes are meant to make the application and workbook version more relevant in the evolving cybersecurity environment as well as easier to use.



## 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 Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC) worked together with the Department of Health and Human Services Office for Civil Rights (OCR), 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 Assistant Secretary for Technology Policy, or The Office for Civil Rights.**

The SRA tool is available for download on ASTP/ONC's website at HealthIT.gov and 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 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 to those businesses. All user-entered data is saved locally in a secure format (only accessible for decryption by the SRA Tool application).

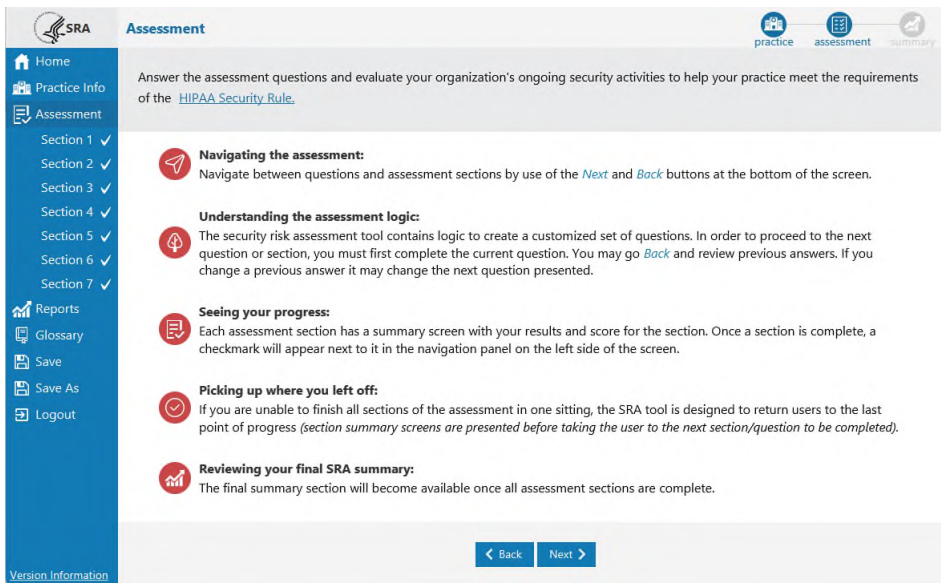
The SRA Tool installer file is available for download from the ASTP/ONC's HealthIT.gov website. It is available at no cost and can be used with Windows 7/8/10/11 operating systems. The SRA Tool installs to the Program Files directory and thus Administrator privileges are required to install.

## 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 seven 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)
- ▲ 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 SRA Tool questionnaire development include:

- ▲ 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 2.0
- ▲ Health Industry Cybersecurity Practices (HICP) Technical Volume 1
- ▲ Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs)

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 allows users to document plans to mitigate identified risks. The tool serves as your local repository for information. Organizations can also link 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 linked to an assessment using the tool's "Add a Document" feature.

Completing a risk assessment requires a time investment and the tool lets you save your progress to be completed later. In addition, you can pause to view your current results at any time during the risk assessment process. The results are available in a color-coded graphic view and printable format.

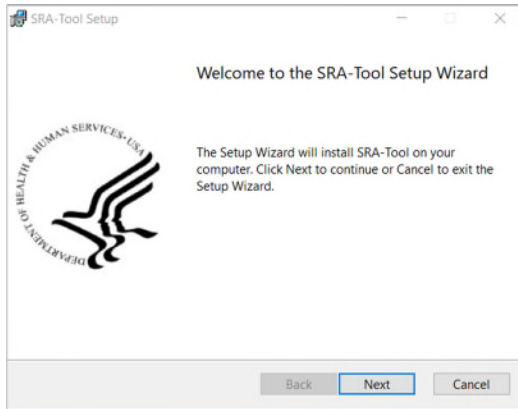
**Need Help? Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.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

## End User Hardware Requirements

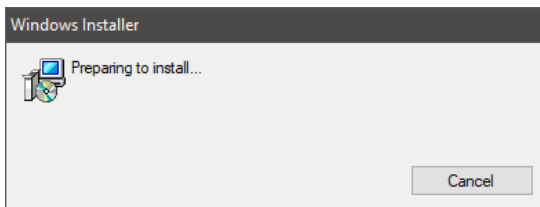
- ▲ Windows 7/8/10/11
- ▲ 2 GHz Pentium processor or better
- ▲ 2 GB RAM or more
- ▲ System type: 64-bit Operating System
- ▲ 1024 x 768 screen resolution or better

## Download Instructions

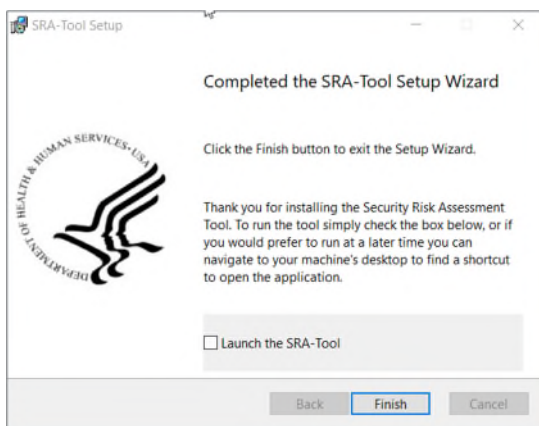
1. Download the installer file from the HealthIT.gov website
  - a. <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment>
  - b. Once downloaded, run the executable to begin installation to your computer. To do this you may need administrative privileges or help from someone with Admin rights from your organization.



2. Click **Next**. You will see a status indicator of the installation progress while the tool is installed on your machine.



3. When installation is complete, click **Finish** in the installation setup wizard.



4. Then locate and double-click the SRA Tool icon on your desktop to begin using the tool.

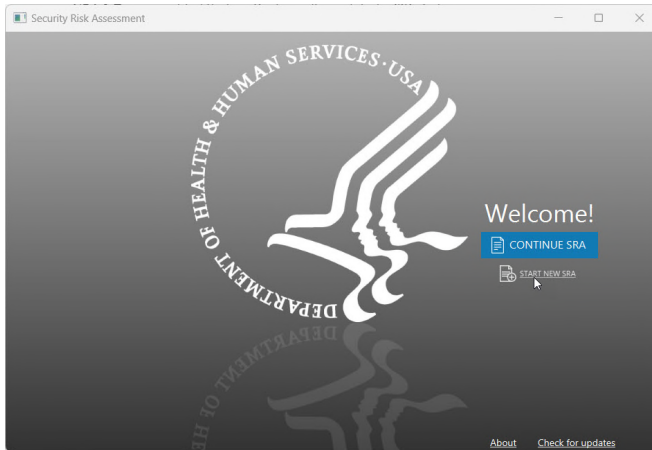
**Note:** The SRA Tool v3.6 is installed to the Program Files directory, which requires administrative privileges. If you are having difficulty installing the tool, you may need to check with your administrator.

# Using The Tool

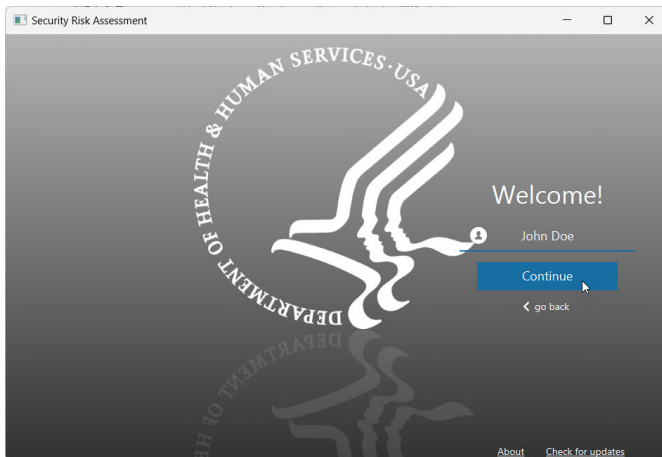
## Starting a New Assessment

To start a new assessment, the SRA Tool must be downloaded and installed on a compatible Microsoft Windows operating system. After application launch, 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.

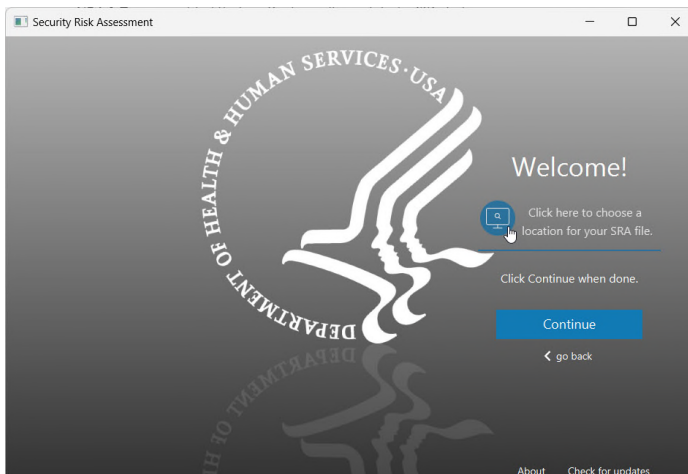
1. Click **START NEW SRA**.



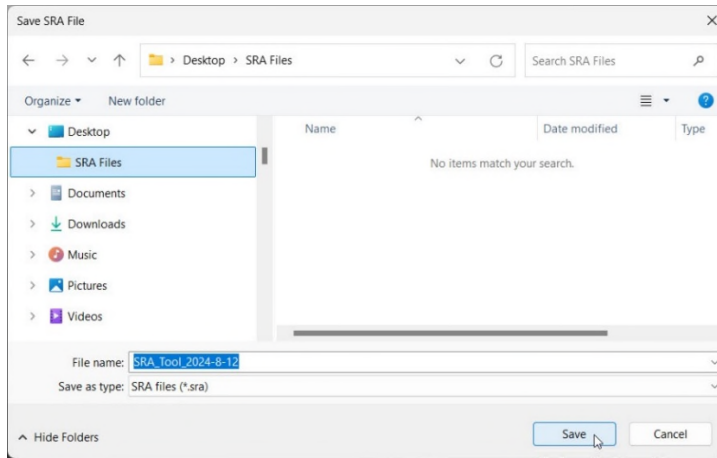
2. Enter a username. This can be a first name, first and last, initials, or anything else to distinguish the current user from other users who may contribute to the risk assessment. Click **Continue**.



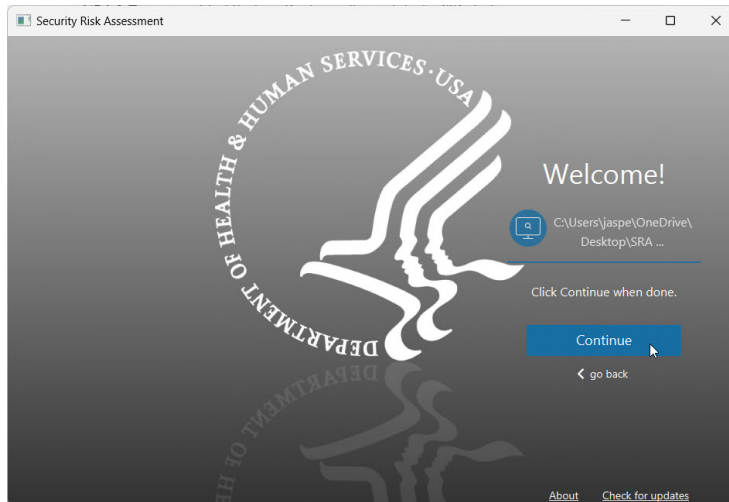
3. Select **Click here to choose a location for your SRA file**. This launches a system file browser.



4. Select a location and file name for the SRA file. 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\_9-3-2025.sra” for example. When done, click **Save**. Remember to note or write down the location on the local network or drive where the file was saved for ease of accessing the file later.



5. Click **Continue** to begin the assessment.




## Continuing an Assessment

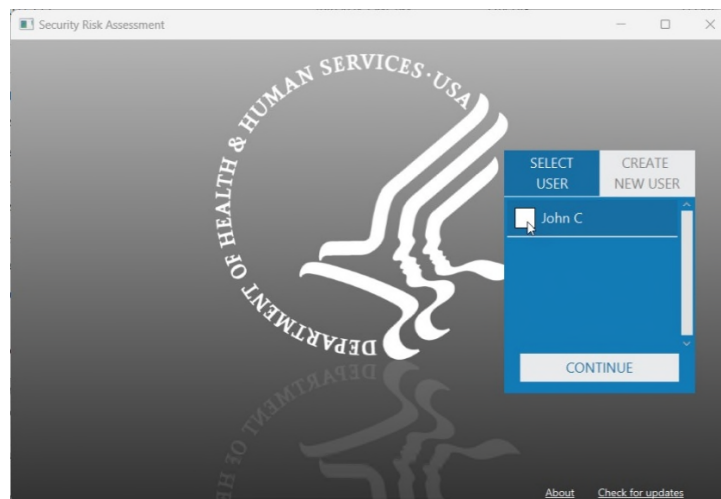
There are two ways to open an existing assessment: double-click on an existing SRA file or launch the SRA Tool and select the assessment to open. Both options are described below. Note that you can open “old” assessments in the new application version of the tool (except for SRA tool v2.0 or older) with SRA Tool 3.6, **but you will not see new questions, new guidance, or new references, which are updates to the “contents.”** See the Version Information section in this User Guide for more details.

### ▲ Option 1: Double-click the SRA file in Windows Explorer

- 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, the “SRA File” file type, and the .SRA extension (file extension may not be displayed depending on OS configuration).

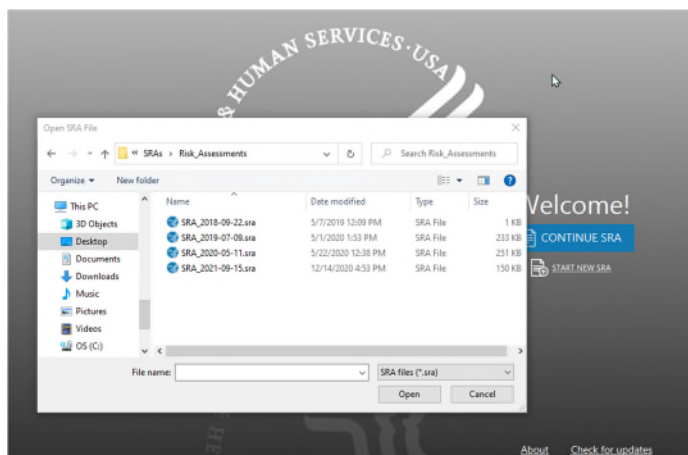
| Name   | Date modified      | Type        | Size   |
|--|--------------------|-------------|--------|
| Archived SRA Files   | 8/13/2024 10:34 AM | File folder |        |
|  SRA_Tool_2023-12-5 | 8/8/2024 10:01 AM  | SRA File    | 365 KB |

- b. Double-click the SRA file.
- c. The SRA Tool application opens the risk assessment as it was last saved, including the user names that created it.
- d. Select an existing user or create a new user, then click **Continue**. The assessment opens and you can review or save changes.

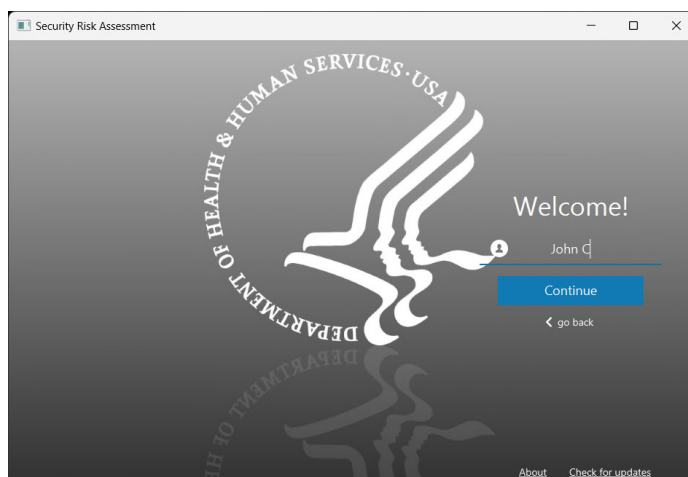


### ▲ Option 2: Open an existing SRA file from within the SRA Tool

- a. Launch the SRA Tool.
- b. Click **CONTINUE SRA**.
- c. Browse to the location with your saved .SRA file (note that you cannot open SRA tool 2.0 files with SRA Tool 3.6 except for bulk uploads of asset and vendor information).
- d. Select the saved assessment SRA file and click **Open**.

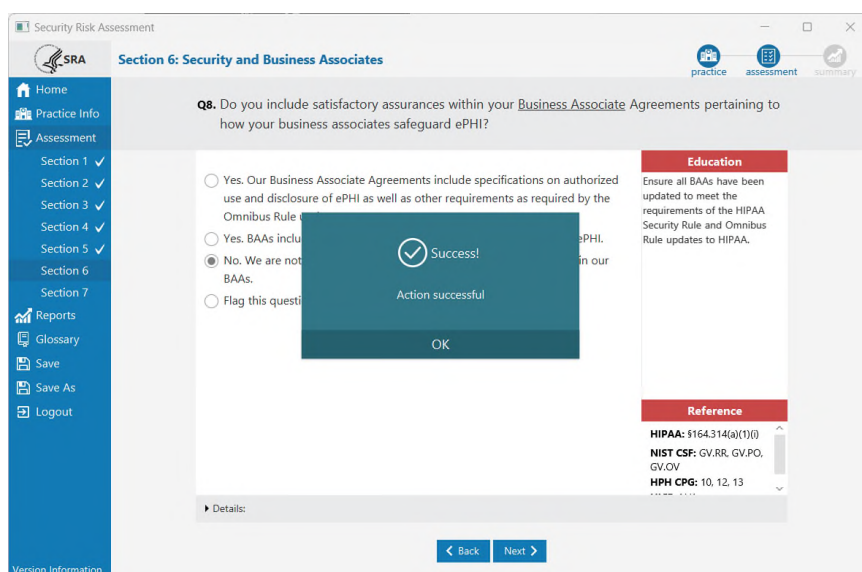


- e. Select an existing user or create a new user, then click **Continue**. The assessment opens and you can review or save changes.



## Saving Assessment Progress

Assessment progress can be saved at any time by clicking **Next** on each screen and by clicking **Save** on the left navigation menu. Progress is saved to the existing file at its current location.



To prevent lost changes, the tool will also confirm if you want 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 within your assessment.

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save

Save As

Logout

SRA

Practice Information

practiceassessmentsummary

Add your [practice information](#) to your security risk assessment.

Consider all contexts of your organization's operations, such as various location(s), department(s), people, and more. Select '+ another location' if you have more than one location.

Practice Name

ABC Inc.

Address

123 Main St.

City, State, Zip

Ann ArborMI48105

Phone, Fax

800-888-8888(000)-0000-0000

Point of Contact

John Appleseed

Title/Role

Administrator

Phone

734-000-0000

Email

John@abc.com

Delete

Save this location

< Back

Next >

Select the **Practice Info** menu to view or enter information. Practice information is included on reports you generate within the SRA Tool.

1. Enter information related to the practice. Click **Save this location** after each practice information section is completed. Note: if you do not click **Save**, you may need to click **Next** twice to both save the information and then advance to the next page.

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 in the assessment. 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 one or more practices. Assets are stored with the assessment data and can be viewed on the Practice Assets screen or by viewing the Detailed Report after an assessment has been completed.

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save

Save As

Logout

SRA

Practice Assets

practiceassessmentsummary

Enter your organization's [assets](#).

Consider all contexts of assets, such as your organization's location(s), department(s), equipment, people, materials, and more.

Want to [add more than one asset](#) at a time?

Add Asset

Download Asset Template

Export Asset List

Upload Asset Template

Total Assets [3]

Manage Assets

ID #

Type

Status

ePHI

Encryption

Assignment

Location

Risk

Manage

Delete

Edit

129011

Laptop

Inactive [Dis...

Receives ePHI

File level encr...

John Applese...

Front Desk

Low

Delete

Edit

129233

Desktop

Not Disposed

Ryan

Hallway

Low

Delete

Edit

199229

Desktop

Active [In-use...

Receives ePHI

Full disk encr...

Wendy K.

Office 2b

Low

Delete

Edit

< Back

Next >

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save

Save As

Logout

SRA

Practice Assets

practiceassessmentsummary

Enter your organization's [assets](#).

Consider all contexts of assets, such as your organization's location(s), department(s), equipment, people, materials, and more.

Want to [add more than one asset](#) at a time?

Add Asset

Download Asset Template

Export Asset List

Upload Asset Template

Total Assets [3]

Manage Assets

ID #

Type

Status

ePHI

Encryption

Assignment

Location

Risk

Manage

Delete

Edit

129011

Laptop

Inactive [Dis...

Receives ePHI

File level encr...

John Applese...

Front Desk

Low

Delete

Edit

129233

Desktop

Not Disposed

Ryan

Hallway

Low

Delete

Edit

199229

Desktop

Active [In-use...

Receives ePHI

Full disk encr...

Wendy K.

Office 2b

Low

Delete

Edit

< Back

Next >

Add Asset

Asset Type

Asset Status

ePHI Access

Asset Disposal

Disposal Date

Asset Encryption

Asset Assignment

Asset Location

Asset ID

Comments

Add

SRA Tool v3.6 User Guide

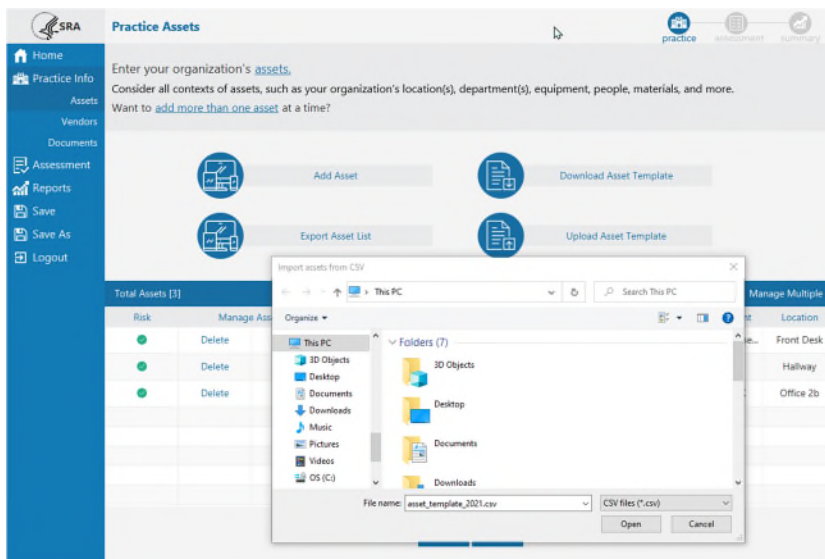
Page | 12

To view or edit Asset information:

1. Select the **Add Asset** button from the Practice Assets page. You can navigate to this page by pressing **Next** after Practice Info or selecting **Assets** under Practice Info 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.
6. 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)

Assets can be added and then exported from the SRA Tool in bulk. This may be helpful in moving your asset list to a new assessment in a later tool version. The Asset template uses a strictly formatted CSV file.



Assets are exported from and imported to the tool with the template. A blank template file can be downloaded from the Practice Assets screen.

|   | 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 |                              |                |           |                                |                             |                       |         |                 |               |

It is important to remember that files must be kept in CSV format to work with the SRA Tool. **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.

1. Select **Export Asset List** from the Practice Assets screen.
2. 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.
3. Select a location and file name for the asset list. Click **Save**.

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

1. Select **Download Asset Template** from the Practice Assets screen.
2. Select a location and file name for the asset template. Click **Save**.

Correctly formatted asset files can be uploaded to the tool as an alternative to manual entry from the 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. Click the **Upload Asset Template** button from the Practice Assets screen
4. Navigate to and select the saved CSV file. Click **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 an SRA file and viewing the Practice Info/Vendors screen or by viewing the Detailed Report after an assessment has been completed.

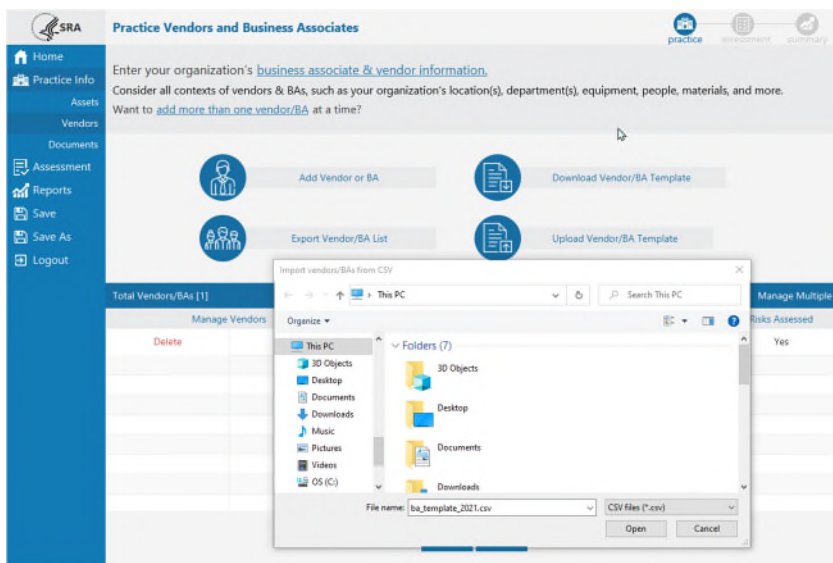
To view or edit Vendor information:

1. Select the **Add Vendor or BA** button from the **Practice Info/Vendors** Page. To access this page, click **Next** after **Practice Info/Assets** or select **Vendors** under **Practice Info** 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. Clicking 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 clicking **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. Clicking **Update** at the bottom of the screen saves changes.
  6. Vendors can be deleted by clicking **Delete** in the vendor row.

## Upload Vendor Template (Bulk Operations)

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 with the template.



A blank template file can be downloaded from the Practice Info/Vendors screen and completed externally before being imported back into an SRA Tool assessment.

|   | 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 Ilc. | laboratory services | 111 Dover Ave.     | Ann Arbor | MI    | 48103   | 734-555-2222 |     |           |         |
| 3 | Cleaners         | cleaning service    | 1909 Washtenaw Ave | Ann Arbor |       |         |              |     |           |         |
| 4 |                  |                     |                    |           |       |         |              |     |           |         |
| 5 |                  |                     |                    |           |       |         |              |     |           |         |
| 6 |                  |                     |                    |           |       |         |              |     |           |         |
| 7 |                  |                     |                    |           |       |         |              |     |           |         |
| 8 |                  |                     |                    |           |       |         |              |     |           |         |
| 9 |                  |                     |                    |           |       |         |              |     |           |         |

It is important to remember that files must be kept in CSV format to work with the SRA Tool. **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. Click **Export Vendor List** from the Practice Info/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. Click **Save**.

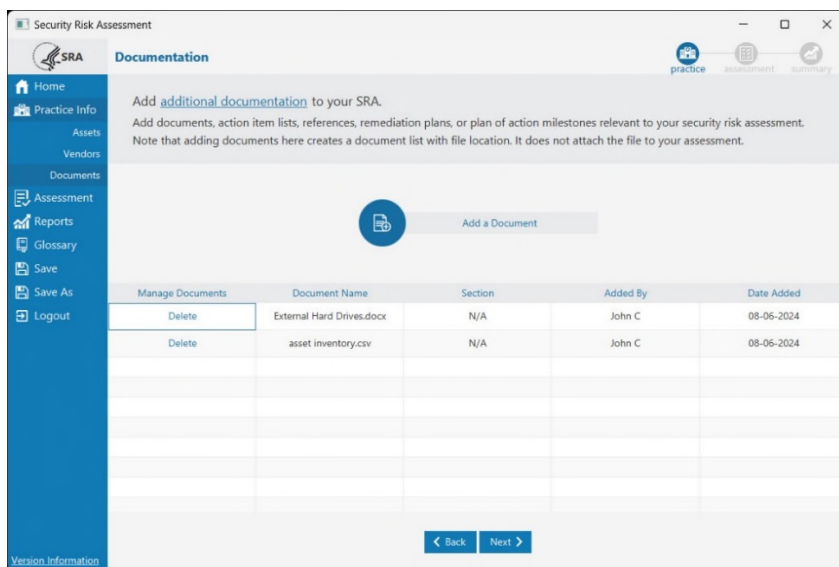
A blank vendor template can be downloaded from the tool if you want to import all vendors from a CSV file.

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

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

## Link Additional Documentation

The Practice Info/Documents screen allows users to link supporting or supplemental documentation to the assessment. No documents are imported into and saved in the SRA tool or the assessment; 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.



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:

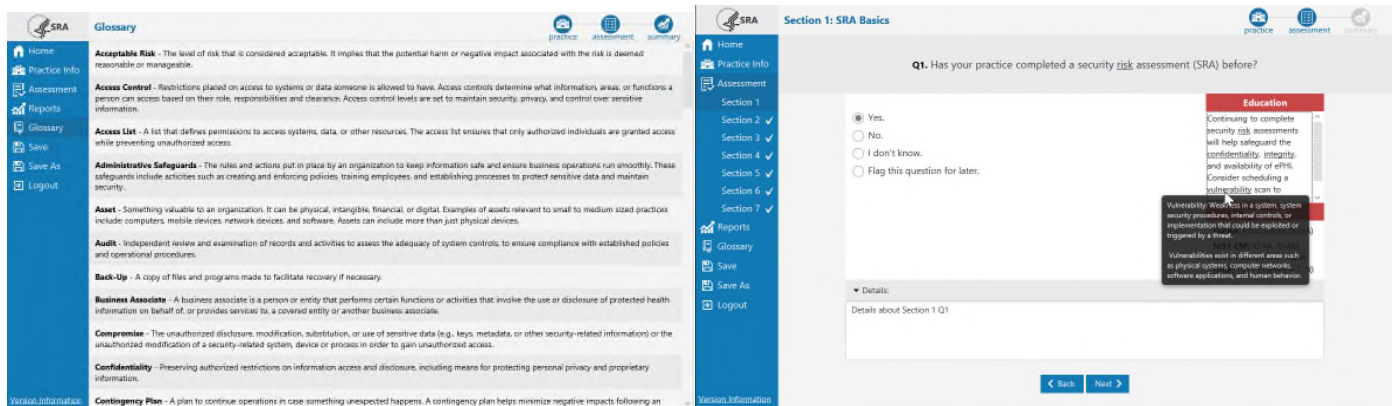
1. Click **Add a Document** at the Practice Info/Documents screen.
2. Browse to the folder location where the document is saved.
3. Select the document file you want linked to the assessment and click **Open**.
4. The file name and the link extension to the documentation will appear in the table below.

The Documentation screen also lists documents that have been added to the assessment from section

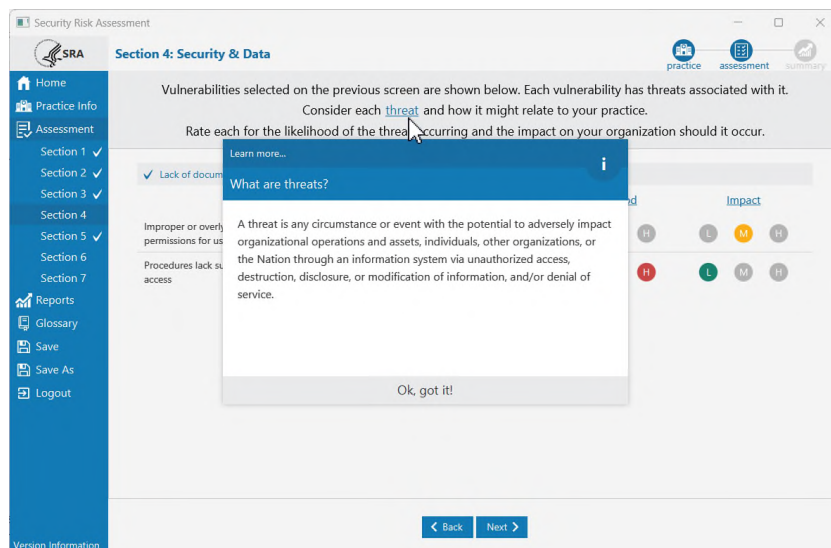
summaries. This is covered in more detail in the Completing an Assessment section.

## 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 that are displayed when a user hovers over an underlined term. Glossary terms in the content can be identified by an underline in the question and education text.

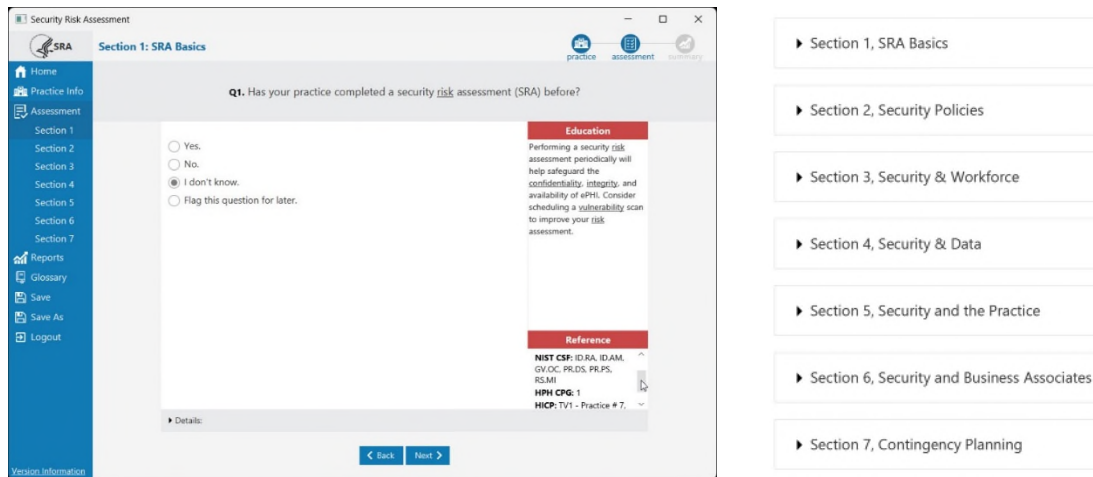


There is blue underlined text in the tool that opens pop-up windows. These may provide richer information on underlined glossary terms and provide hyperlinks to external content. Click **Ok, got it!** to close pop-ups.



## Completing an Assessment

The assessment portion of the tool is arranged into sections and the list can be seen on the left side of the screen while completing assessments.



Each section contains branching logic that can omit questions based on your previous responses. Because of this, you may see different questions when you complete an SRA if your answers change.

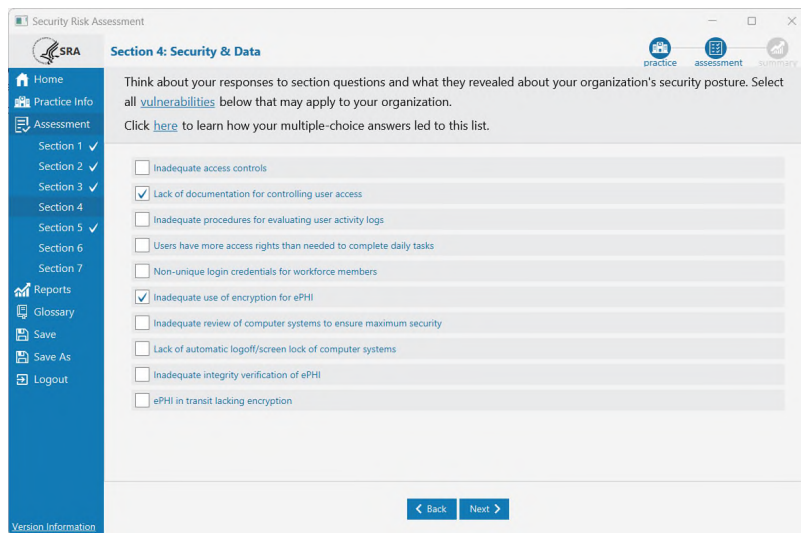
- ▲ Each question in the assessment portion is a single answer and multiple choice. This means that one answer and only one answer must be answered to continue.
- ▲ The question number is displayed to the left of the question text. Questions are numbered starting at “Q1” for each section.
- ▲ If you select “Flag this question for later” you can skip the question, but should return to it eventually and select another response. The tool provides a “Flagged Report” that lists all question flagged for later, but that report is for reference purposes only and you cannot change your answer from that report.
- ▲ The **Education** panel on the right side of the screen shows information relevant to your selected answer. When no answer is selected, the panel is blank. Once a selection is made, information relevant to that selection is displayed.
- ▲ The **Reference** panel is on the lower right below Education and shows references to relevant security information for the question. Click on the references to copy the reference text or get more information on the reference types. Doing the latter opens a popup window that describes the reference set (e.g., HIPAA, NIST CSF, HPH CPG, HICP) and provides a link to it.
- ▲ The **Details** box can be used to enter supporting information or notes about an individual question. This free text field can be expanded and collapsed by clicking **Details**.
- ▲ Clicking **Next** at the bottom of the screen saves your input and advances to the next question or section. After each multiple-choice section, users are prompted to select vulnerabilities that apply and rate the associated threats.

## Threat & Vulnerability Rating

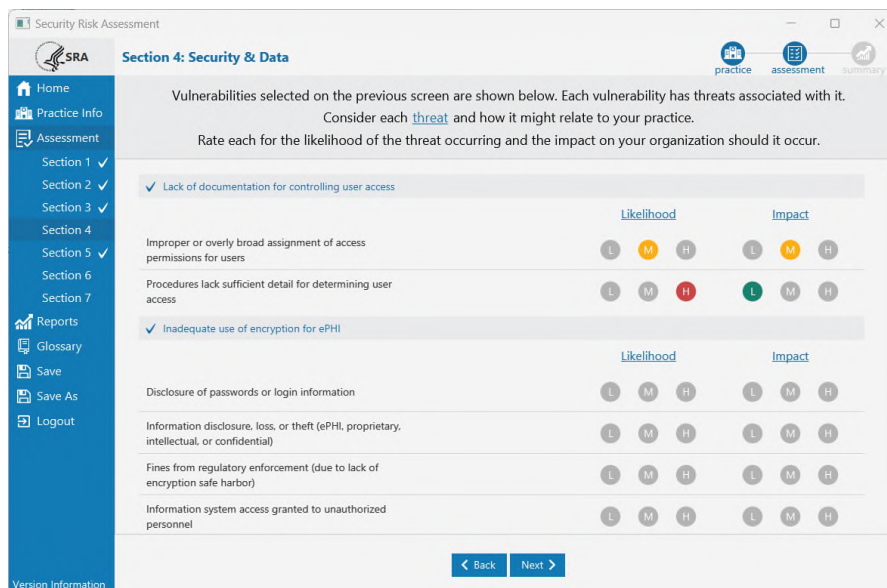
After completing each section of multiple-choice questions, a set of vulnerabilities is presented. Multiple items can be selected.

Select each vulnerability applicable to your practice.

1. Check the check box next to each applicable vulnerability.



2. Select **Next** to continue.
3. Each selected vulnerability has associated threats. Each threat must be rated based on the likelihood of occurrence at the practice and the impact it would cause. Rate the **Likelihood** and **Impact** for each threat listed, where L = Low, M = Moderate, and H = High. Note that you may need to scroll down to see all rows. In SRA Tool 3.6, “Medium” has been changed to “Moderate.” In the screen capture below, the first set of threats have been rated and show the selected rating color, but the second set still need to be rated.



**Likelihood rating guidance:** This is your judgment on the likelihood of “undesirable events”—such as power outage, theft, or fire—to occur within your practice.

**Low (L):** a modest or insignificant chance of occurrence. Shows as green.

**Moderate (M):** a significant chance of occurrence. Shows as yellow.

**High (H):** a probable chance of occurrence. Shows as red.

**Impact rating guidance:** This is your judgment on the damage of “undesirable events”—such as power outage, theft, or fire—if they were to occur within your practice.

**Low (L):** a modest disruption with minor impact. Shows as green.

**Moderate (M):** a significant disruption with some damage. Shows as yellow.

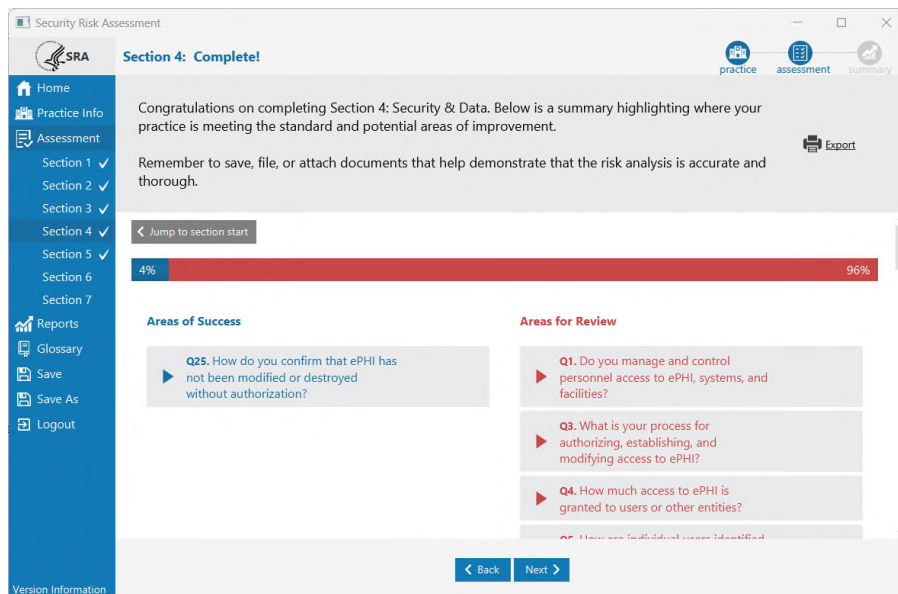
**High (H):** a catastrophic disruption with consequential damage. Shows as red.

- Both Likelihood and Impact must be rated **for each threat listed** at this screen before you can continue.
- Click **Next** to continue. If a warning appears, scroll down through each threat and rate any that were missed.

## Section Complete Summary

A section summary appears for each completed section and highlights areas of success and areas for review. Sections are completed when all multiple-choice questions are answered, vulnerabilities for the section topic are selected, and all resulting threats are rated. The screen also lets you export the section summary.

At the bottom of the screen are two features for saving section-specific details. There is a text field for entering information and—new in version 3.6—a button to let users confirm that all section questions are accurate.



The Section Complete screen shows the following information and options:

- ▲ **Areas of Success** presents a list of questions where responses met the expectation, indicating compliance.
- ▲ **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.
- ▲ Clicking on the triangle on the left side of each question expands a tile revealing the chosen response and education information.
- ▲ The bar in the center of the screen represents the percentage of responses in the **Areas of Success** and **Areas for Review** categories.
- ▲ The **Export** button near the top right corner of the screen can be used to export a PDF copy of the current section summary.
- ▲ 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

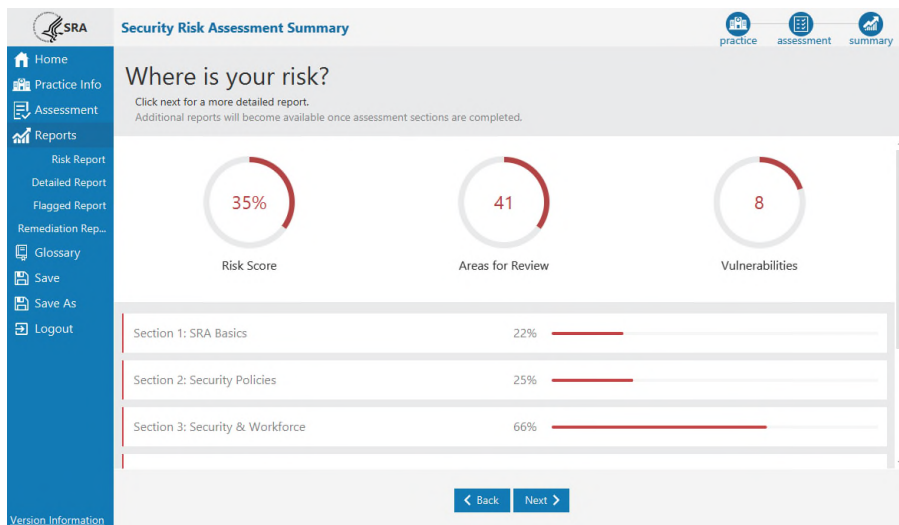
completed section are preserved when using this feature, but you will need to advance through the questions again.

- ▲ The **Section Reviewed/Confirmed** button can be used to signify supervisory approval of an entire section or that all responses in the section have been reviewed and are confirmed as accurate. Clicking this button saves the current user name and date and adds the confirmation to the Detailed Report PDF. As with the **Additional Information** field, it is important to click **Next** to save any changes to this screen.
- ▲ The **Additional Information** field can be used to store details or other information you wish to associate with the current section. Click **Next** to save changes. Stored text is added to the Detailed Report PDF.
- ▲ Click the **+Documents** button at the bottom of the Section Complete screen to reference related documents. Browse to the location where the document file is saved. Select the document you want linked to this assessment section and click **Open**. The file name and location will appear in the table for this section and in the documents table at the Practice Info/Documents screen. Click **Next** to save changes.

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.

## Security Risk Assessment Summary

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

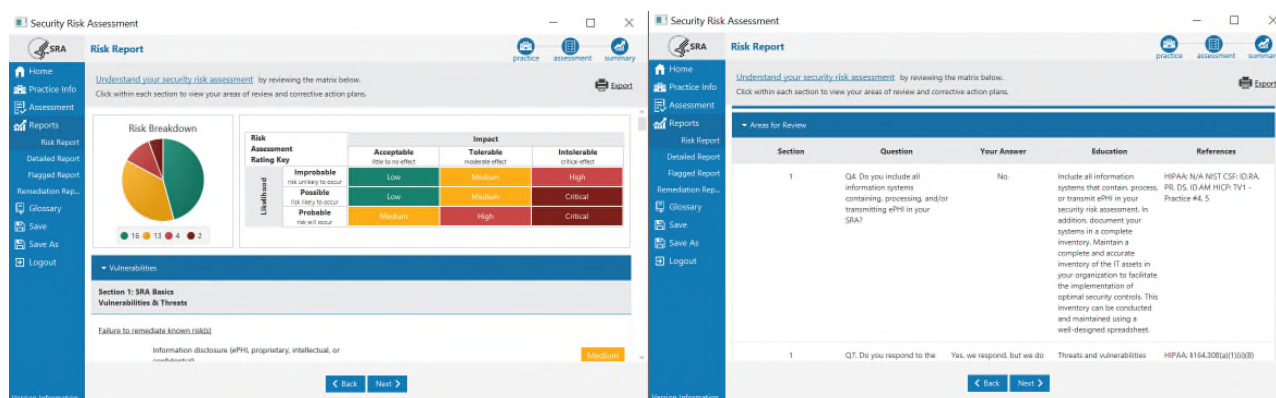


The Security Risk Assessment Summary shows the following information and options:

- ▲ **Risk Score** – percentage of responses sorted into Areas for Review across the whole assessment.
- ▲ **Areas for Review** – count of responses sorted into the Areas for Review category.
- ▲ **Vulnerabilities** – count of vulnerabilities selected as applicable to the practice.
- ▲ **Section risk scores** – a percentage of responses sorted into Areas for Review for each section. Scroll down to see the risk score for all sections.

## Risk Report

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



The Risk Report shows the following information and options:

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

## Detailed Report

The Detailed Report is an output of all assessment information entered into the SRA Tool, with the following exceptions: comments entered at the Section Complete screens and the Practice Info/Documents list are not included.

| 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 |

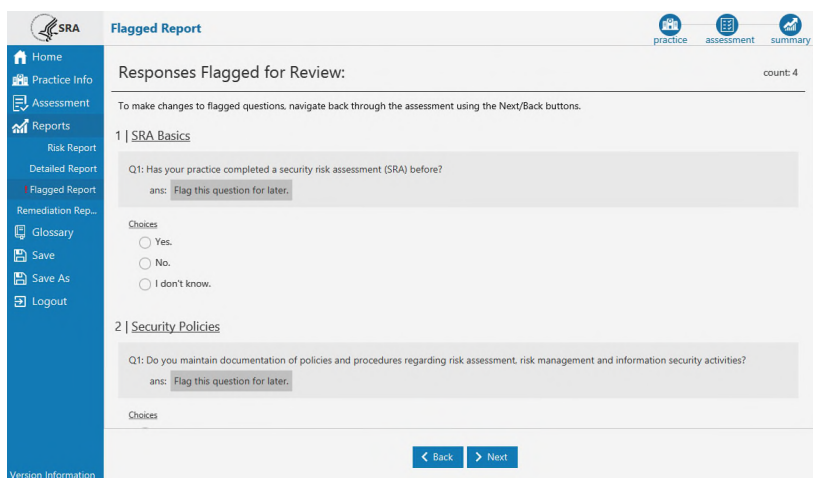
Each section is broken down into threats & vulnerabilities and multiple choice.

- ▲ Each section is collapsible. Select the section title or black triangle to expand a section. Click again to collapse.
- ▲ **Risk Score**—the percentage of multiple-choice responses sorted into Areas for Review—is displayed for each section.
- ▲ **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.
- ▲ Practice information, asset information, and business associates and vendors are all displayed at the bottom of the Detailed Report.
- ▲ Click **Export Options** at the top right corner of the Detailed Report to download the report. You can export this report as a PDF or Excel workbook.

## Flagged Report

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

**The Flagged Report is not interactive and merely provides a summary.**



To make changes to responses shown in the Flagged Report, you need to navigate back through the assessment.

1. Click on the **Assessment** menu and then the section you will change.
2. If this takes you to the section start, click **Next** until you reach the question you wish to change. If clicking on a section takes you to the Section Summary (i.e., the end), click **Back** until you reach the question and response you would like to change.
3. Upon changing your response, click **Next** to view the next sequence of questions which is required to complete the section again. Note that a change in a flagged question 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.

The screenshot displays the SRA Remediation Report interface. On the left is a navigation menu with options: Home, Practice Info, Assessment, Reports, Risk Report, Detailed Report, Flagged Report, Remediation Rep..., Glossary, Save, Save As, and Logout. The main content area is titled 'Remediation Report' and includes a description: 'The Remediation Report provides a space to record responses to deficiencies in process or policies identified in your risk assessment. Items for review can be assigned an owner, due date, and date completed. [Learn more about documenting remediations...](#)'. Below this is a 'Sections' selector showing a sequence of numbered tabs (1-7) and the text 'now showing Section 2, (5) records'. The current section is 'Section 2: Security Policies'. It contains a question: 'Q3: How do you update your security program documentation, including policies and procedures?'. The answer states: 'We update policies and procedures ad hoc, for example when an immediate need prompts the change.' Under 'Education', it says: 'You should conduct periodic reviews of information security policies and update them as needed. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.' A 'References' section lists: 'HIPAA: §164.316(b)(2)(iii)', 'NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS, ID.IM', 'HPH CPG: 4', and 'HICP: TV1 - Practice # 10'. Below the references is a large text area for 'Remediation Activities:'. At the bottom, there are input fields for 'Owner:', 'Due Date:', and 'Date Completed:', followed by a '+ Link Document' button and a 'Save Remediation' button. A '< Back' button is at the very bottom.

The Remediation Report shows the following information and options:

- ▲ **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.
- ▲ **Remediation Activities** – Text area to be used for documenting response to risk identified for each question in the report.
- ▲ **Owner** – Text field to assign an owner for the remediation activity. This is a way of indicating responsibility for improving response to risk.
- ▲ **Due Date** – Date field that may be used to track deadlines to respond to risk.
- ▲ **Date Completed** – Date field used to track when a remediation activity is completed.
- ▲ **+ Link Documentation** – Allows linkage to documentation on a local or network drive.
- ▲ **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**.

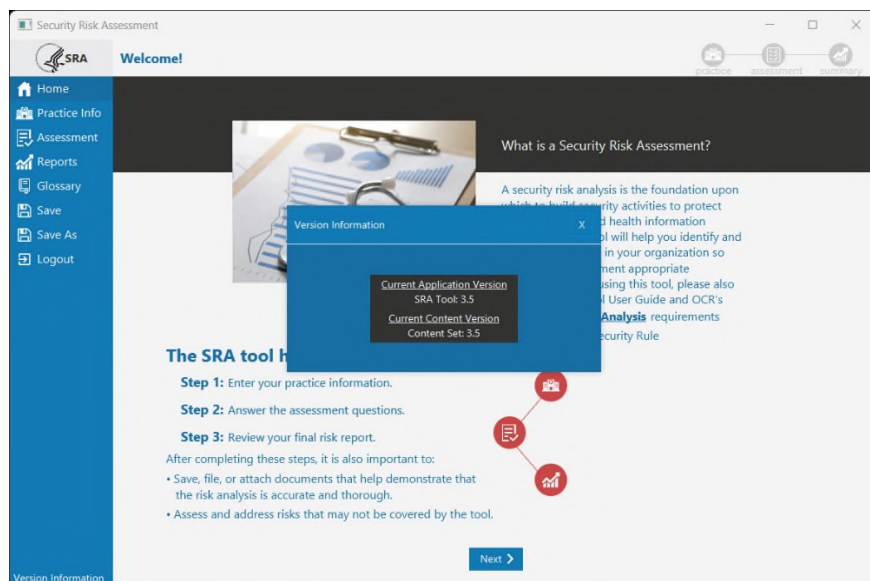
## Saving & Exporting

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

- ▲ **Save Detailed Report as PDF or Excel.** The Detailed Report is a complete output of assessment information captured by the tool, minus linked documents. It contains Practice Information, Assets, Vendors, multiple choice questions and answers, vulnerabilities, and threats. The Detailed Report can be downloaded as a PDF or Excel by clicking **Export Options** near the top right corner of the Detailed Report screen. The Excel version does not include all information provided in the PDF version.
- ▲ **Export Section Summaries.** You can download a PDF of each section's questions and responses. To do this, go to the Section Complete page of each section.
- ▲ **Export Remediation and Risk Reports.** These reports can be downloaded as PDFs.
- ▲ **Export Asset List.** Asset information from your assessment can be exported as a CSV file by selecting **Export Asset List** from the Assets screen under Practice Info. This is a useful method to move assets from one SRA file to another without re-entering each one individually.
- ▲ **Export Vendor List.** Vendor information from your assessment can be exported as a CSV file by selecting **Export Vendor/BA List** from the Vendors screen under Practice Info. This is a useful method to move vendor information from one SRA file to another without re-entering each one individually.
- ▲ **Copy Education and Reference Text.** Within the assessment you can click on Education and Reference text to copy it to your clipboard. You can then Paste it into other applications. You can also copy and paste this information from the Detailed Report Excel version.

## Version Information

There are two types of versions in the SRA Tool: the application version and the content version. These can be viewed by clicking **Version Information** at the bottom left on the SRA Tool page.



### SRA TOOL APPLICATION VERSION

The SRA Tool version is the release number of the SRA Tool application. 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:

- ▲ **Check for updates** link on the SRA Tool Welcome Screen. Located in the bottom right corner of the screen before login.
- ▲ **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.

## SRA TOOL CONTENT VERSION

Content version refers to the questions, education, references, and glossary information in the tool since these can be updated with an SRA Tool application release or separately.

The content version does not need to match the SRA Tool version. For example, you may open an assessment (SRA File) created with SRA Tool version 3.4 in SRA Tool version 3.6. In this case, you will see the 3.4 content in the 3.6 application; the assessment is not upgraded when opened with a later version of the tool. Since Content Version 3.6 includes five new assessment questions and new references—including HPH CPGs—that were added in version 3.5, these will not be shown when using Content version 3.4. Content version 3.6 also includes significant changes to content text and removes one question that was deemed to be duplicative. The only way to see the latest content changes are by installing the latest application version and beginning a new assessment. As noted above, continuing an existing assessment created in a previous version will only show the previous content.

## 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 is available for users unable to install the desktop application version. It contains the same multiple-choice questions, education, references, and risk score system but in a workbook format. The Excel workbook version can be downloaded from the HealthIT.gov SRA Tool page.

<https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

| Section 1 - SRA Basics |  |           |                               |   |                |           |  |
|------------------------|--|-----------|-------------------------------|---|----------------|-----------|--|
| Question #             | Question Text  | Indicator | Question Responses            | Education   | 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 a vulnerability scan to assist in identification of technical vulnerabilities to improve your risk assessment.              |                | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 7, 10 |
| 5                      |  | ✓         | No.                           | Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to assist in identification of technical vulnerabilities to improve your risk assessment. | Review         | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 7, 10 |
| 6                      |  |           | 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 assist in identification of technical vulnerabilities to improve your risk assessment. |                | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 7, 10 |
| 7                      |  |           | 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)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 7, 10 |
| 2                      | Do you review and update your SRA?                                   |           | Yes.                          | This is the most effective option to protect the confidentiality, integrity, and availability of ePHI. Include language in your policies and procedures to review and update your risk assessment regularly.  |                | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 10    |
| 11                     |  | ✓         | No.                           | Consider reviewing and updating your security risk assessment periodically. Include language in your policies and procedures to review and update your risk assessment regularly.   |                | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 10    |
| 12                     |  |           | I don't know.                 | Consider reviewing and updating your security risk assessment periodically. Include language in your policies and procedures to review and update your risk assessment regularly.   |                | Required  | HIPAA: §164.308(a)(1)(ii)(A)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI<br>HPH CPG: 1<br>HICP: TV1 - Practice # 10    |
| 13                     |  |           | 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)<br>NIST CSF: ID.RA, ID.AM, GV.DC, PR.DS, PR.PS, RS.MI   |

Example screen capture of the assessment questions (top of Section 1 tab)

| Section 1 - SRA Basics |  |           |  |           |            |          |            |
|------------------------|--|-----------|--|-----------|------------|----------|------------|
| Question #             | Question Text  | Indicator | Question Responses   | Education | Likelihood | Impact   | Risk Score |
| 74                     | Threats & Vulnerabilities                            |           |  |           |            |          |            |
| 75                     | Inadequate risk awareness or failure to identify new |           | Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches      |           | Low        | Low      | Low        |
| 76                     |  |           | Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.) |           | Low        | Moderate | Moderate   |
| 77                     |  |           | Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or destruction from  |           | Low        | High     | High       |
| 78                     |  |           | Man-made threat(s) such as insider carelessness, theft/vandalism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals                                       |           | Moderate   | High     | Critical   |
| 79                     |  |           | Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions               |           | High       | High     | Critical   |
| 80                     |  |           |  |           |            |          |            |
| 81                     | Failure to remediate known risk(s)                   |           | Information disclosure (ePHI, proprietary, intellectual, or confidential)  |           | Low        |          |            |
| 82                     |  |           | Penalties from contractual non-compliance with third-party vendors   |           |            |          |            |
| 83                     |  |           | Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems  |           | Moderate   |          |            |
| 84                     |  |           | Data deletion or corruption of records   |           | High       |          |            |
| 85                     |  |           | Prolonged exposure to hacker, computer criminal, malicious code, or careless insider   |           |            |          |            |
| 86                     |  |           | Corrective enforcement from regulatory agencies (e.g., HHS, OCR, FTC, CMS, State or Local jurisdictions)   |           |            |          |            |
| 87                     |  |           | Hardware/equipment malfunction   |           |            |          |            |
| 88                     |  |           |  |           |            |          |            |
| 89                     | Failure to meet minimum regulatory requirements and  |           | Corrective enforcement from regulatory agencies (e.g., HHS, OCR, FTC, CMS, State or Local jurisdictions)   |           |            |          |            |
| 90                     |  |           | Damage to public reputation due to breach  |           |            |          |            |
| 91                     |  |           | Failure to attain incentives or optimize value-based reimbursement   |           |            |          |            |
| 92                     |  |           | Litigation from breach victims due to lack of reasonable and appropriate safeguards  |           |            |          |            |
| 93                     |  |           |  |           |            |          |            |
| 94                     | Inadequate Asset Tracking                            |           | Information disclosure (ePHI, proprietary, intellectual, or confidential)  |           |            |          |            |
| 95                     |  |           | Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems  |           |            |          |            |
| 96                     |  |           | Unauthorized use of assets or changes to data within information systems   |           |            |          |            |
| 97                     |  |           | Unauthorized installation of software or applications  |           |            |          |            |
| 98                     |  |           | Loss, theft, or disruption of assets   |           |            |          |            |
| 99                     |  |           | Improper operation/configuration of assets   |           |            |          |            |
| 100                    |  |           |  |           |            |          |            |
| 101                    | Unspecified workforce security responsibilities      |           | Non-remediated weaknesses  |           |            |          |            |
| 102                    |  |           | Prolonged duration of addressing non-remediated weaknesses   |           |            |          |            |
| 103                    |  |           | Insider carelessness exposing ePHI or causing disruption to information systems and business processes   |           |            |          |            |
| 104                    |  |           |  |           |            |          |            |
| 105                    |  |           |  |           |            |          |            |
| 106                    |  |           |  |           |            |          |            |
| 107                    |  |           |  |           |            |          |            |
| 108                    |  |           |  |           |            |          |            |
| 109                    |  |           |  |           |            |          |            |
| 110                    |  |           |  |           |            |          |            |

Example screen capture of the Threats & Vulnerability scoring (bottom of Section 1 tab)

Instructions for using the SRA Tool Excel Workbook version:

- ▲ Worksheets for all seven SRA Tool sections are included. Each sheet should be reviewed to complete a risk assessment.

- ▲ Use the File/Save As feature in Excel to create working versions (i.e., files) from the blank template. If your installation of Excel asks you to confirm or enable editing, choose yes. This allows you to make selections in cells.
- ▲ Select question responses using the dropdown in the **Response Indicator** column in the row that corresponds to the desired response. Responses are marked using the “✓” symbol.
- ▲ Responses indicating “areas for review” are automatically highlighted in yellow. Responses indicating “areas of success” are not highlighted in any color.
- ▲ The Threats & Vulnerabilities section at the bottom of each sheet contains a list of vulnerabilities related to that section and their associated threats. Rate threats for vulnerabilities that are applicable to your organization based on the **Likelihood** of a threat occurring and the **Impact** it would have on your organization should it occur.
- ▲ 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 (FAQs)

---

### 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 summary reports?

To access the reports available under the Reports menu, the assessment must be 100% completed. Once a section is completed, a white check mark appears next to its name in the menu. You can select, review, and download reports when all sections have check marks. Note that individual section reports can be downloaded from each Section Complete screen before all sections are completed.

### 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 and who modified it. This timestamp will not update unless the response is changed. In 3.6 you can now attest that all questions in a section are reviewed and confirmed. By clicking the **Section Reviewed/Confirmed** button on each Section Complete screen, you can now confirm an approval date and user name in your Detailed Report PDF.

### 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. If 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 **Save As** 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 **Save As** 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. ***In SRA Tool 3.6, you can now attest that all questions in a section are reviewed and confirmed.*** To do this go to each Section Complete page and click the **Section Reviewed/Confirmed** button at the bottom of the screen. You will be asked to confirm that all questions within the section have been reviewed or updated. By clicking **OK**, you are attesting that the assessment is accurate in its current state. The review/confirmation date and user name appears in the Detailed Report PDF for each section where this attestation is added.

### **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 **Assessment** 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 backward 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 TEFCA? The TEFCA references 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 TEFCA rule is finalized.

### **Is video help available?**

A video recording of the SRA Tool webinar is available on HealthIT.gov in the **SRA Webinar** section. <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

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

Results from independent penetration testing can be uploaded/linked 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 3<sup>rd</sup> 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 ASTP/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 ASTP/ONC.

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

To make changes to responses shown in the Flagged 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 backward until you reach the desired question or the “Jump to section start” button to move to the beginning of the section and navigate forward using the Next button.

When you have moved backward from the Section Summary of a completed section, the white check mark signifying section completion is removed. 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](http://HealthIT.gov)