

The Security Risk Assessment Tool

Overview for Small and Medium Practices

Presenters: Dawn Bishop, John Christensen,
Nick Heesters, Mauricio Lovelace



Agenda

- What is a Security Risk Assessment?
- Overview of the SRA Tool
- Enhancements in Version 3.6
- Q&A

What is Security Risk Assessment?

A covered entity or business associate must:

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the organization”

HIPAA § 164.308(a)(1)(ii)(A)

The HIPAA Security Rule requires covered entities to:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce.

Risk Analysis components of a Security Risk Assessment:

- Identifying all ePHI within your organization.
- Identifying sources of ePHI
- Identifying human, natural, and environmental threats to information systems that contain ePHI.

Outcomes from security risk assessment

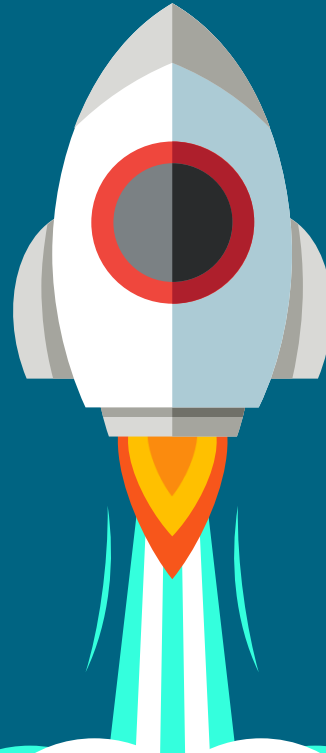
Organizations can use information from their assessment to inform decisions regarding security measure implementations to:

- Design personnel screening processes
- Identify and strategize data backup
- Determine where and how encryption should be used
- Determine what authentication may be required to protect data integrity
- Determine which policies and procedures may need to be created or improved to protect ePHI



Challenge

- Organizations are vulnerable
 - SRA is required
- Small budgets, few staff



SRA Tool

An accessible, wizard-based tool to aid in the identification and assessment of risks to ePHI.

The SRA Tool

Risk Assessment

SRA

Section 1: SRA Basics

practice assessment summary

Home

Practice Info

Assessment

Section 1

Section 2 ✓

Section 3 ✓

Section 4 ✓

Section 5 ✓

Section 6 ✓

Section 7 ✓

Reports

Glossary

Save

Save As

Logout

Version Information

Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?

☐ Written and verbal communication as well as coordinated corrective action planning.

☒ Written communication only.

☐ Verbal communication only.

☐ We do not communicate risk assessment results to workforce members.

☐ Flag this question for later.

Education

Written results of your SRA should be communicated to the personnel responsible for responding to identified threats and vulnerabilities but also consider involving the personnel responsible for responding to identified threats and vulnerabilities in the creation of corrective action plans.

Reference

HIPAA: §164.308(a)(1)(ii)(B)

NIST CSF: ID.RA, ID.RM, RS.MI

HICP: N/A

Details:

< Back

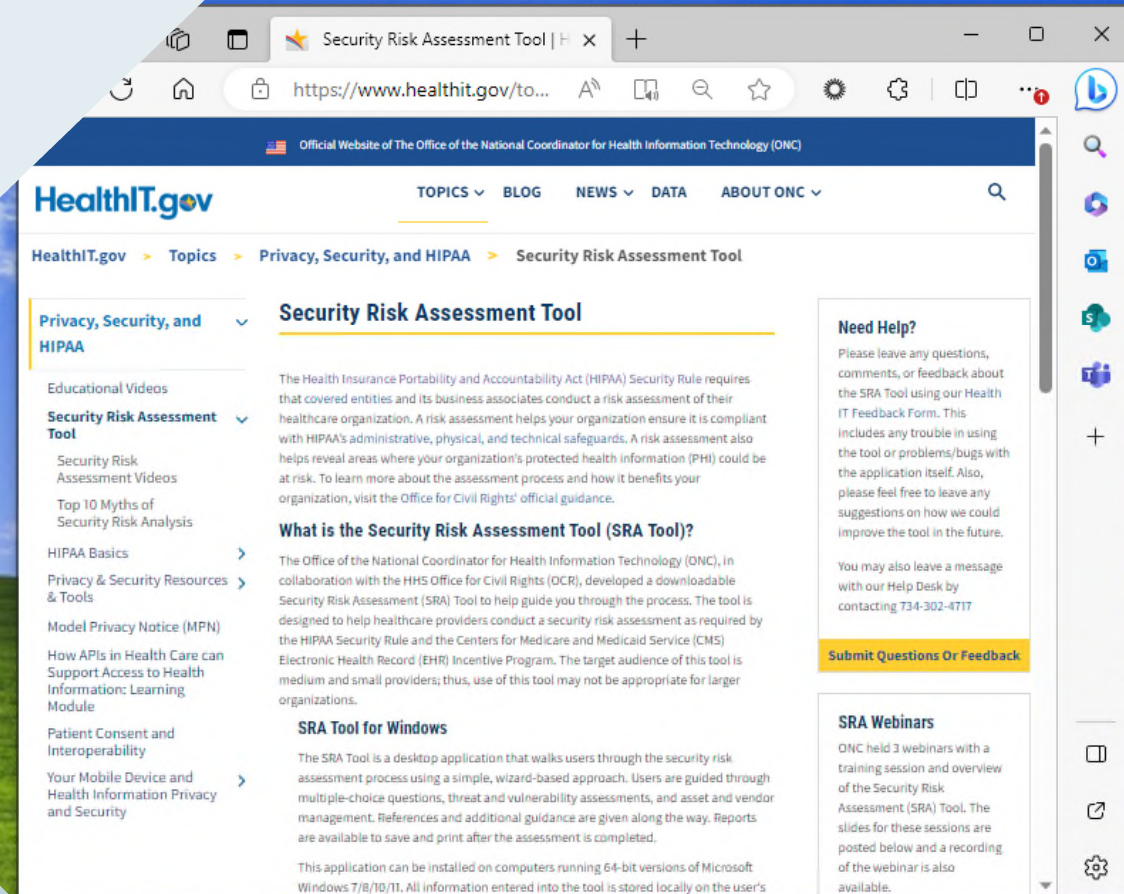
Next >

Content

The SRA Tool's content was developed using the following sources:

- ▲ HIPAA Security Rule
- ▲ National Institute of Standards and Technology (NIST) Special Publication 800-66
- ▲ NIST Special Publication [Guide to Implementing FISMA Security Controls] 800-53
- ▲ NIST Special Publication [Guide to Assessing FISMA Controls] 800-53A
- ▲ Health Information Technology for Economic and Clinical Health (HITECH) Act
- ▲ Assessment questions will reference NIST Cybersecurity Framework guidance
- ▲ Health Industry Cybersecurity Practices (HICP)
- ▲ Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs)

Downloading, Installing, and Using the SRA Tool



The screenshot shows a web browser window displaying the HealthIT.gov website. The browser's address bar shows the URL <https://www.healthit.gov/to...>. The page header includes the HealthIT.gov logo and navigation links for TOPICS, BLOG, NEWS, DATA, and ABOUT ONC. The main content area is titled "Security Risk Assessment Tool" and is part of a breadcrumb trail: HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool. A left sidebar contains a list of links under the "Privacy, Security, and HIPAA" category, with "Security Risk Assessment Tool" highlighted. The main content area provides an overview of the tool, explaining its purpose and how it helps healthcare organizations comply with HIPAA's Security Rule. It also includes a section titled "What is the Security Risk Assessment Tool (SRA Tool)?" and a "SRA Tool for Windows" section. A right sidebar contains a "Need Help?" section with contact information and a "Submit Questions Or Feedback" button, as well as a "SRA Webinars" section.

Security Risk Assessment Tool | x

https://www.healthit.gov/to...

Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

HealthIT.gov

TOPICS ▾ BLOG NEWS ▾ DATA ABOUT ONC ▾

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA ▾

- Educational Videos
- Security Risk Assessment Tool** ▾
 - Security Risk Assessment Videos
 - Top 10 Myths of Security Risk Analysis
- HIPAA Basics >
- Privacy & Security Resources & Tools >
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module
- Patient Consent and Interoperability
- Your Mobile Device and Health Information Privacy and Security >

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the Office for Civil Rights' official guidance.

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's

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.

You may also leave a message with our Help Desk by contacting 734-302-4717

[Submit Questions Or Feedback](#)

SRA Webinars

ONC held 3 webinars with a training session and overview of the Security Risk Assessment (SRA) Tool. The slides for these sessions are posted below and a recording of the webinar is also available.

Privacy, Security, and HIPAA ▾

Educational Videos

Security Risk Assessment Tool ▾

Security Risk Assessment Videos

Top 10 Myths of Security Risk Analysis

HIPAA Basics >

Privacy & Security Resources & Tools >

Model Privacy Notice (MPN)

How APIs in Health Care can Support Access to Health Information: Learning Module

Patient Consent and Interoperability

Your Mobile Device and Health Information Privacy and Security >

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the [Office for Civil Rights' official guidance](#).

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's computer. HHS does not collect, view, store, or transmit any information entered into the SRA Tool.

[Download Version 3.6 of the SRA Tool for Windows \[.msi – 73.1 MB\]](#)

SRA Tool Excel Workbook

This version of the SRA Tool takes the same content from the Windows desktop app, presents it in a familiar spreadsheet format. The Excel Workbook contains conditional formatting and formulas to calculate and help identify risk in a similar fashion to the SRA Tool application. This version of the SRA Tool is intended to replace the legacy "Paper Version" and may be a good option for users who do not have access to Microsoft Windows or otherwise need more flexibility than is provided by the SRA Tool for Windows.

This workbook can be used on any computer using Microsoft Excel or another program capable of handling .xlsx files. Some features and formatting may only work in Excel.

[Download Version 3.6 of the SRA Tool Excel Workbook \[.xlsx – 141 KB\]](#)



Download & Installation

The tool can be downloaded from [HealthIT.gov](https://healthit.gov). The downloaded file is the tool installer. Double click to run the installer and walk through the install steps. Once downloaded, a blue “SRA-Tool” icon will appear on your desktop.

The SRA Tool runs on Windows 8, 10, and 11. All information entered into the tool is contained locally. No information is transmitted to DHHS, ASTP/ONC, or OCR.

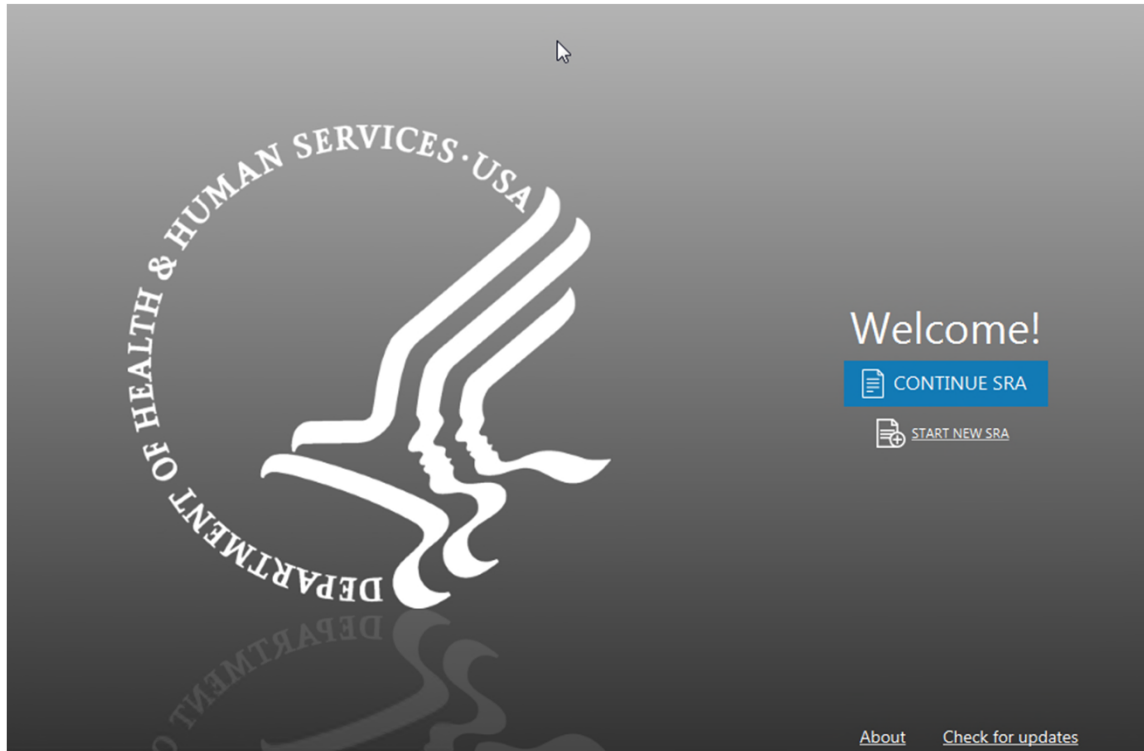
Note: Users must have administrative privileges to install the SRA Tool. For this reason, you may need help from your IT department or system administrator to install the tool. Admin privileges are not needed to run the tool once it has been installed. Instructions on reviewing the digital certificate is covered in a later slide.

Welcome Screen

Select “Start New SRA” to begin a new assessment or “Continue SRA” to open an existing assessment file.

The “Check for Updates” link helps you confirm what version of the application and content you are using.

Note: You should only install SRA Tool updates downloaded from the HealthIT.gov SRA Tool page.





Welcome!

Enter your name

Continue



Welcome!

John Doe

Continue

< go back

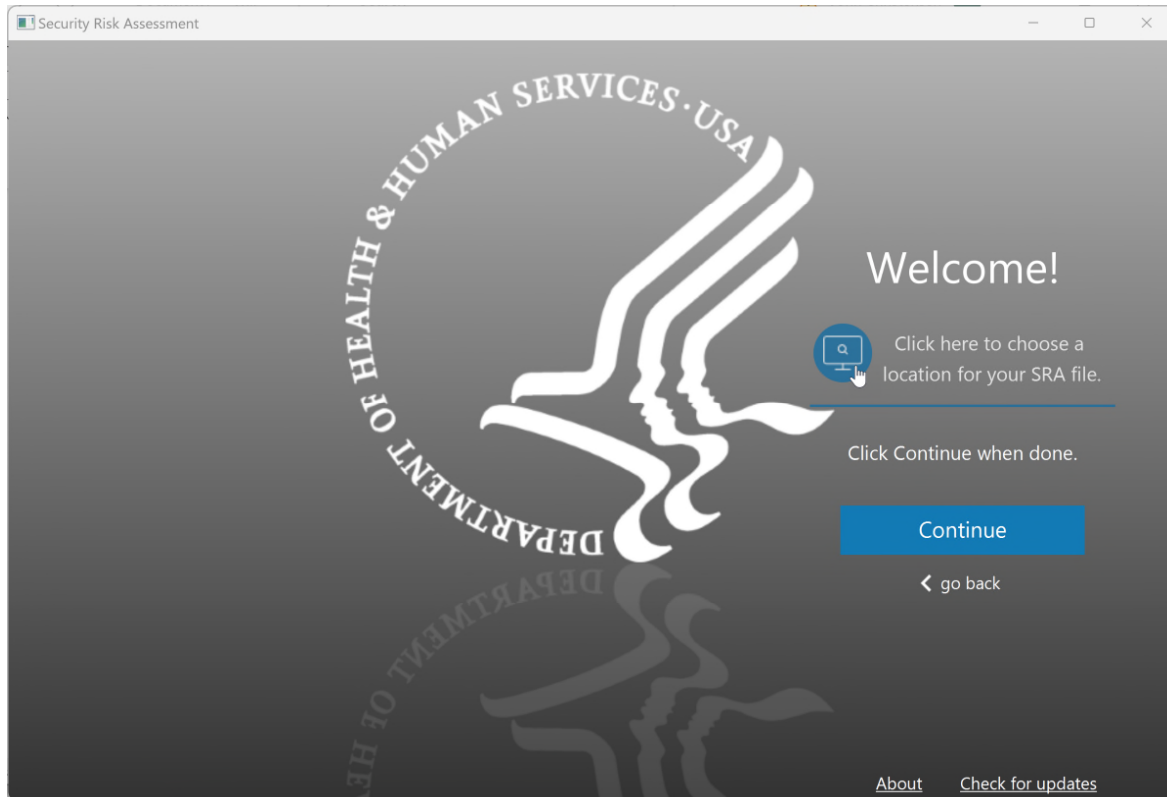
[About](#) [Check for updates](#)

Entering a Username

When beginning a new assessment, the user is asked to enter their name. A full first and last name is recommended.

The SRA Tool supports multiple user accounts, so more than one person can work on an SRA file in progress.

When opening an existing assessment, the user will need to select their username or create a new one.



Saving a New SRA File

The SRA Tool creates SRA files that can only be opened with the SRA Tool application.

After entering your name, you then select a file name and save location for the new .SRA file.

Files with the .SRA extension can be opened and edited only with the SRA Tool application.

The screenshot displays the Altarum SRA application interface. The left sidebar contains navigation links: Home, Practice Info, Assets, Vendors, Documents, Assessment, Reports, Glossary, Save, Save As, and Logout. The main content area is divided into two sections: 'Practice Information' and 'Practice Assets'.

Practice Information Section:

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.

Fields for Practice Information:

- Practice Name
- Address
- City, State, Zip
- Phone, Fax
- Point of Contact
- Title/Role
- Phone

Practice Assets Section:

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?

Buttons for Practice Assets:

- Add Asset
- Download Asset Template
- Export Asset List
- Upload Asset Template

Assets Table:

Total Assets [0] Manage Multiple

Risk	Manage Assets	ID #	Type	Status	ePHI	Encryption	Assignment	Location
No content in table								

Navigation buttons: < Back, Next >

Practice Information, Asset & Vendor Management

Begin assessments by gathering and entering information, including:

- Practice locations
- Assets (computers, equipment, other hardware)
- Business Associates (vendors)
- Relevant policy, procedure, training, and other documents

Security Risk Assessment

SRA

Section 2: Security Policies

practice assessment summary

Home Practice Info Assessment

Section 1 ✓ Section 2 Section 3 Section 4 Section 5 Section 6 Section 7

Reports Glossary Save Save As Logout

Version Information

Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?

☐ Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.
 ☒ Yes, we have some documentation for our information security and risk management activities, but not all of our policies and procedures are documented.
 ☐ No, we do not maintain documentation on our information security activities or risk management.
 ☐ Flag this question for later.

Education

You should document policies and procedures to ensure you consistently make informed decisions on the effective monitoring, identification, and mitigation of risks to ePHI. Establishing and implementing cybersecurity

Reference

HIPAA: §164.316(a)
NIST CSF: GV.RR, GV.PO, GV.OV, ID.RA, PR.PS
HPH CPG: 1, 14, 15
HIP: TV1 - Practice # 10

▼ Details:

The Details section can be expanded to enter notes or supporting information about the question or response.

< Back Next >

Assessment

The Assessment section contains seven sections with multiple-choice questions and branching logic.

The Education panel provides guidance related to each response given.

The Reference panel links each question to a HIPAA Security Rule citation.

Progress indicators are provided in the navigation panel as sections are completed.

Section 2: Security Policies

Think about your responses to section questions and what they revealed about your organization's security posture. Select all [vulnerabilities](#) below that may apply to your organization.

Click [here](#) to learn how your multiple-choice answers led to this list.

- ☐ Failure to update Policies & Procedures
- ☒ Failure to share security procedure information with appropriate parties
- ☒ Inconsistent/unclear risk management documentation
- ☐ No risk management documentation (or low retention of documentation)

Vulnerabilities selected on the previous screen are shown below. Each vulnerability has threats associated with it.

Consider each [threat](#) and how it might relate to your practice.

Rate each for the likelihood of the threat occurring and the impact on your organization should it occur.

Vulnerability	Likelihood			Impact		
✓ Failure to share security procedure information with appropriate parties						
Unauthorized access to ePHI or sensitive information permitted	L	M	H	L	M	H
Disruption of information system function	L	M	H	L	M	H
ePHI accessed by unauthorized entities	L	M	H	L	M	H
Insider carelessness causing disruption	L	M	H	L	M	H
Insider carelessness exposing ePHI	L	M	H	L	M	H
✓ Inconsistent/unclear risk management documentation						
Unclear security coordination across workforce	L	M	H	L	M	H

[Back](#) [Next](#)

Threats & Vulnerabilities

At the end of each section of multiple-choice questions, users are asked to select from a list of vulnerabilities that may be applicable to their practice.

Each vulnerability that is selected comes with a list of related threats that must be rated for:

- The **likelihood** of occurring and
- The **impact** should it occur.

Your threat ratings here will be shown as a risk score on the Risk Report.

Security Risk Assessment

SRA

Section 2: Complete!

practice assessment summary

Home Practice Info Assessment

Section 1 ✓ Section 2 ✓ Section 3 Section 4 Section 5 Section 6 Section 7

Reports Glossary Save Save As Logout

Version Information

Congratulations on completing Section 2: Security Policies. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

Remember to save, file, or attach documents that help demonstrate that the risk analysis is accurate and thorough.

Export

< Jump to section start

37% 63%

Areas of Success

Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?

Q2. Do you review and update your security documentation, including policies and procedures?

Q4. Is the security officer involved in all

Areas for Review

Q3. How do you update your security program documentation, including policies and procedures?

Q5. How does documentation for your risk management and security procedures compare to your actual business practices?

Q6. How long are information security

Section Reviewed/Confirmed

Reviewed By: John Doe Review Date: Tue Sep 09 13:50:06 EDT

Additional Information (Click Next to save any changes at this page)

Documents

< Back Next >

Section Summary

Each section is concluded with a **Section Summary** that shows the questions, responses selected, and education content.

Questions are divided into **Areas of Success** and **Areas for Review** based on your responses:

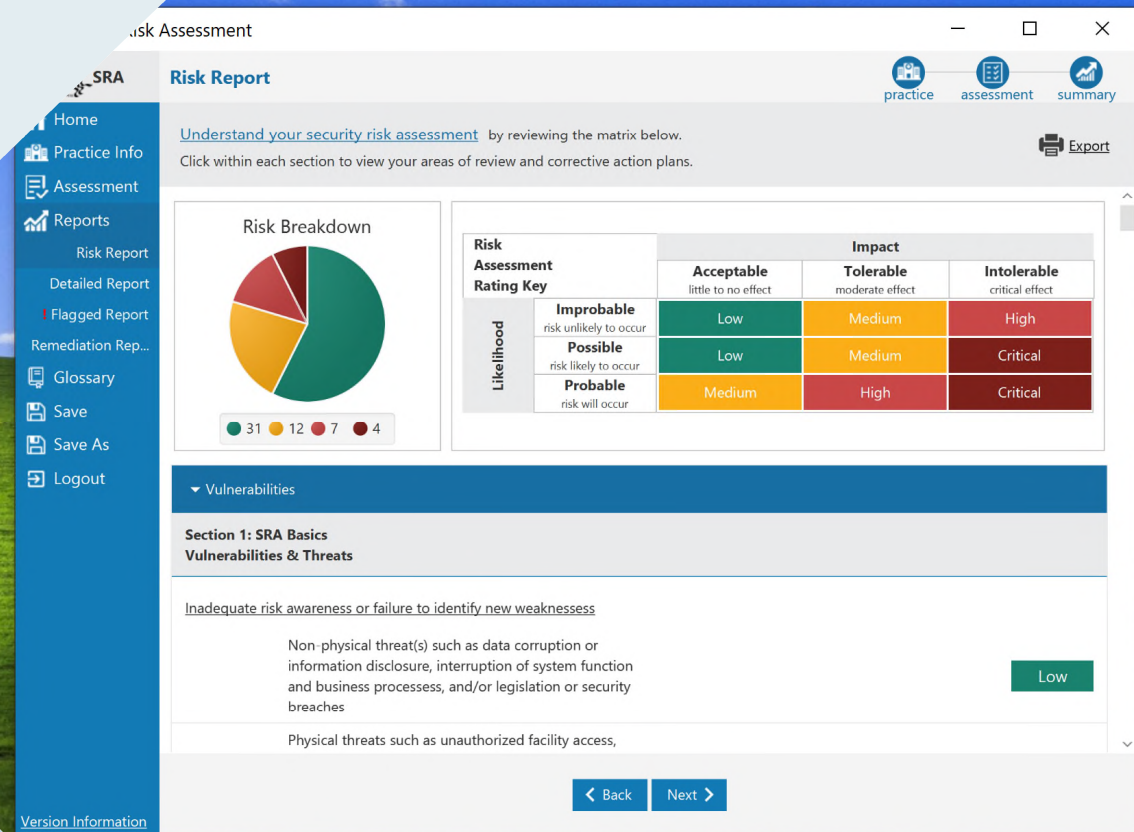
- **Areas of Success** are responses that represent the highest level of compliance.
- **Areas for Review** represent responses that could use improvement.

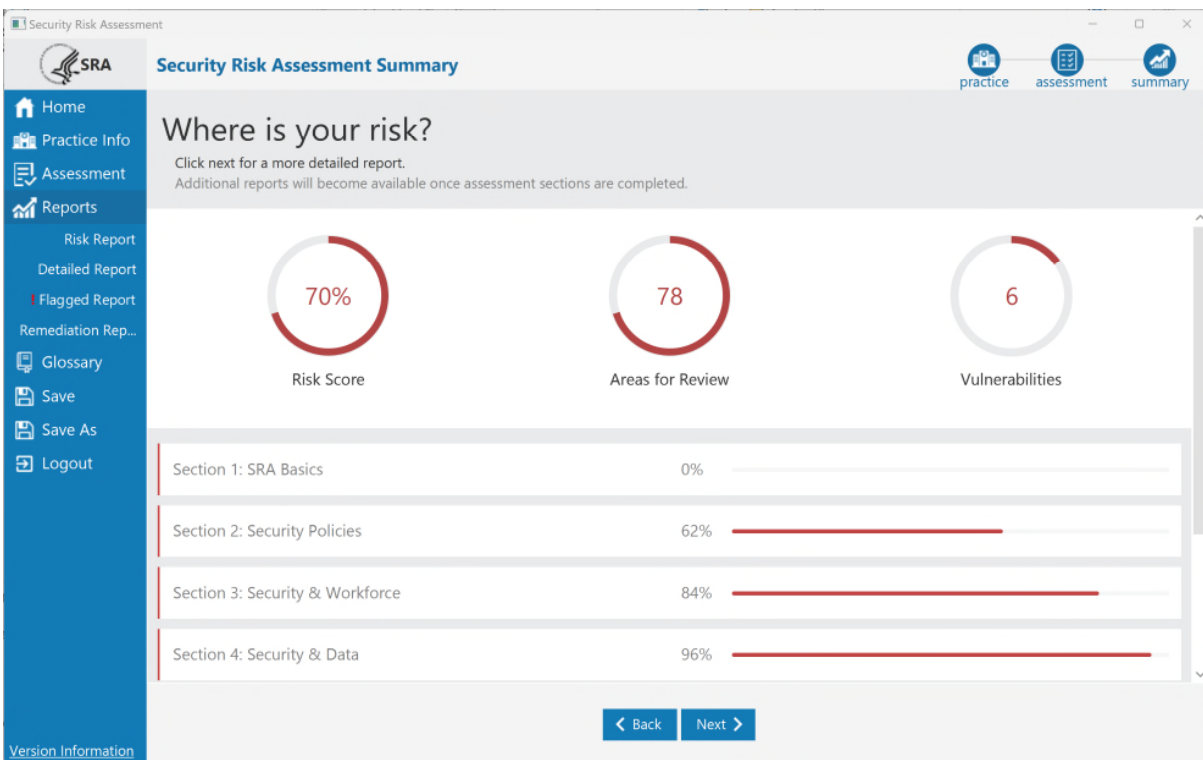
Users can also:

- Indicate section **approval** (*new in 3.6*)
- Add **Additional Information** specific to each section
- Add/link **relevant documents** necessary to demonstrate accuracy and thoroughness of section responses

Click **Next** to save entries or confirmation here.

Reports





Summary Report

Reports are available only after all Assessment sections are completed.

The Summary Report is high level summary of your risk assessment.

- **Risk Score** shows the percentage of all questions in your assessment sorted into **Areas for Review**.
- **Areas for Review** shows the number of all questions in your assessment sorted into **Areas for Review**.
- **Vulnerabilities** shows the total number of vulnerabilities selected as applicable to the practice or organization.

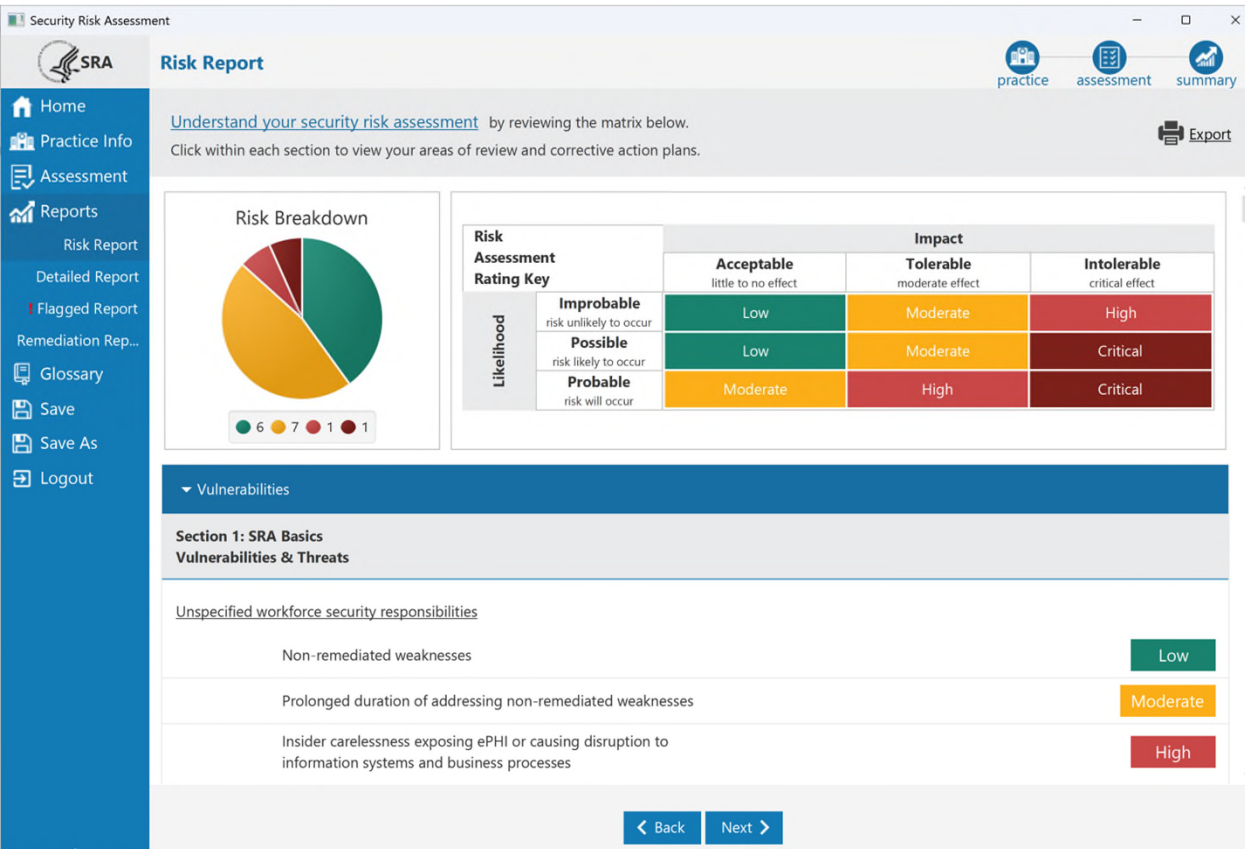
The Risk Scores for individual assessment sections are also shown.

Risk Report

The Risk Report identifies all areas of risk across your assessment.

- **Risk Breakdown** shows a sum of threat ratings in each risk level (Low, Moderate, High, and Critical).
- The **Risk Assessment Rating Key** shows how likelihood and impact ratings combine to rate risk levels.

The **Vulnerability** section lists each vulnerability selected during the assessment with its rated risk level.



Risk Report (*continued*)

The Risk Report also summarizes all questions that were sorted into Areas for Review.

- Users can review questions, selected answers, and corresponding education guidance on how to improve security and mitigate risk in that area.
- Relevant references are also provided for each question in the Risk Report.

Security Risk Assessment

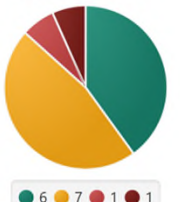
Risk Report

practice assessment summary

Export

Understand your security risk assessment by reviewing the matrix below.
Click within each section to view your areas of review and corrective action plans.

Risk Breakdown



6 7 1 1

Risk Assessment Rating Key

		Impact		
		Acceptable little to no effect	Tolerable moderate effect	Intolerable critical effect
Likelihood	Improbable risk unlikely to occur	Low	Moderate	High
	Possible risk likely to occur	Low	Moderate	Critical
	Probable risk will occur	Moderate	High	Critical

► Vulnerabilities

▼ Areas for Review

Section	Question	Your Answer	Education	References
1	Q1. Has your practice completed a security risk assessment (SRA) before?	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	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, GV.OC, PR.DS, PR.PS, RS.MI HPH CPG: 1 HICP: TV1 - Practice # 7, 10

< Back Next >

Version Information

Detailed Report

Security Risk Assessment

Detailed Report

Click each section to expand and review more details.

practice assessment summary

Export Options

▼ Section 1, SRA Basics Risk Score: 100%

Threats & Vulnerabilities Risk Rating

Unspecified workforce security responsibilities

Non-remediated weaknesses	Low
Prolonged duration of addressing non-remediated weaknesses	Moderate
Insider carelessness exposing ePHI or causing disruption to information systems and business processes	High

Question	Answer	Education	References	Compliance Guidance/Rule	Username	Date/Time
Q1. Has your practice completed a security risk assessment (SRA) before?	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	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, GV.OC, PR.DS, PR.PS, RS.MI HPH CPG: 1 HICP: TV1 - Practice # 7, 10	Required	JSC	Fri Aug 22 11:22:11 EDT 2025

< Back Next >

Version Information

The **Detailed Report** is a collection of all data captured throughout the entire assessment, including:

- All questions and responses, including the username with date/time stamp
- Each threat and vulnerability rating
- Practice Information including Assets and Vendors
- Additional information or approvals entered for each section.

Users can export a PDF or Excel copy of the report from this screen.

Remediation Report

This report lists all areas of risk identified in your assessment and provides space to plan remediation activities, including:

- Enter comments, notes, or plans to respond to each risk
- Assign an owner
- Assign a due date
- Mark the date completed
- Link relevant policy or other documents

The screenshot shows the 'Remediation Report' page in the Security Risk Assessment (SRA) application. The interface includes a left sidebar with navigation links: Home, Practice Info, Assessment, Reports, Risk Report, Detailed Report, Flagged Report, Remediation Rep..., Glossary, Save, Save As, Logout, and Version Information. The main content area is titled 'Remediation Report' and contains 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 section navigation bar with tabs for Sections 1 through 7, with Section 2 selected and showing 5 records. The main content area is divided into three sections: 'Answer' (text input), 'Education' (text input), and 'References' (list of references). The 'Answer' section contains the text: 'We update policies and procedures ad hoc, for example when an immediate need prompts the change.' The 'Education' section contains the text: '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.' The '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 these sections is a 'Remediation Activities' section with a large text input area. At the bottom, there are fields for 'Owner', 'Due Date', and 'Date Completed', each with a dropdown menu. To the right of these fields are links for '+ Link Document' and 'Save Remediation'. A 'Back' button is located at the bottom left of the main content area.

Excel Workbook

The interactive workbook includes worksheets for each of the seven sections of the SRA Tool. This includes the same questions, answers, and education from SRA Tool application.

Users can also indicate the likelihood and impact of threats for each vulnerability.

This option provides cross-platform support to users unable to install or use the application. It may also be helpful to users who want to copy text from questions, responses, and education.

The workbook version is available for download from the HealthIT.gov SRA Tool page.

Section 1 - SRA Basics						
Question #	Question Text	Indicator	Question Responses	Guidance	Risk Indicated	Required?
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.		Required
			No.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI.	Review	Required
			I don't know.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI.		Required
			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
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.		Required
			No.	Consider reviewing and updating your security risk assessment periodically.		Required
			I don't know.	Consider reviewing and updating your security risk assessment periodically.		Required
			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
NOTES:						
Threats & Vulnerabilities						
1	Inadequate risk awareness or failure to identify new				Likelihood	Impact
			Non-physical threat(s) such as data corruption or		Low	Medium
			Physical threats such as unauthorized facility		Low	Low
			Natural threat(s) such as damage from		Low	Low
			Man-Made threat(s) such as insider carelessness,		Medium	Medium
			Infrastructure threat(s) such as building/road		High	High
2	Failure to remediate known risk(s)					
			Information disclosure (ePHI, proprietary,		Low	Low
			Penalties from contractual non-compliance with		Low	Medium
			Disruption of business processes, information		Medium	Medium
			Data deletion or corruption of records		Low	High
			Prolonged exposure to hacker, computer criminal,		Low	Low
			Corrective enforcement from regulatory agencies		Low	Low
			Hardware/equipment malfunction			
3	Failure to meet minimum regulatory requirements and security standards					
			Corrective enforcement from regulatory agencies		Low	Low
			Penalties from contractual non-compliance with		Medium	Medium

What to Expect

- Invest a significant amount of time.
- The value of the SRA to your organization depends on the integrity of the input.
- Spend time on understanding requirements, security, where ePHI exists within your organization's IT environment, and what threats to consider.
- Ensure an inclusive scope. This means considering risks and vulnerabilities to ePHI throughout the organization wherever it is created, maintained, received, or transmitted.
- Regarding applications, be sure to look beyond just the EHR system.
 - *For example: Practice management, scheduling, billing, telecommunications, e-mail, cloud apps, and other platforms can all contain or access ePHI*

Enhancements in Version 3.6

The screenshot displays the 'Remediation Report' window within a 'Risk Assessment' application. The interface features a blue sidebar with navigation 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...](#)' and an 'Export' button. Below this is a 'Sections' navigation bar with tabs 1 through 7, currently showing 'Section 1, (3) records' and '0/3 Remediations Completed - Section 1'. The main content area is divided into two sections: 'Section 1: SRA Basics' and 'Section 2: SRA Basics'. Each section contains a question (Q3 and Q4), an 'Answer' field, an 'Education' field, and a 'References' field. The 'Add Remediation' button is located at the bottom of the first section, and the 'Back' button is at the bottom of the second section. The 'Version Information' link is visible in the bottom left corner of the sidebar.

Risk Assessment

SRA

Remediation Report

practice assessment summary

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...](#) Export

Sections: < 1 2 3 4 5 6 7 > now showing Section 1, (3) records 0/3 Remediations Completed - Section 1

Section 1: SRA Basics

Q3: How often do you review and update your SRA?

Answer: Only in response to operational changes and/or security incidents.

Education
An accurate and thorough security risk assessment should be reviewed and updated periodically, or in response to operational changes, or security incidents.

References
HIPAA: §164.308(a)(1)(ii)(A)
NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR.IP, RS.MI
HICP: N/A

Add Remediation

Q4: Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?

Answer: No.

Education
Include all information systems that contain, process, or transmit ePHI in your security risk assessment. In addition, document your systems in a complete inventory. Maintain a complete and accurate inventory of the IT assets in your organization to facilitate the implementation of optimal

References
HIPAA: N/A
NIST CSF: ID.RA, PR.DS, ID.AM
HICP: TV1, Practice # 5

Back

Version Information

Section review and confirmation

Each of the seven sections now has a **Section Reviewed/Confirmed** button at the section summary page.

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.

This may be useful when updating last year's SRA to confirm the responses are still accurate.

Note: It's important to click **Next** to save changes made here.

Security Risk Assessment

SRA

Section 7: Complete!

practice assessment summary

Home Practice Info Assessment

Section 1 ✓ Section 2 ✓ Section 3 ✓ Section 4 ✓ Section 5 ✓ Section 6 ✓ Section 7 ✓

Reports Glossary Save Save As Logout

Version Information

Congratulations on completing Section 7: Contingency Planning. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

Remember to save, file, or attach your risk analysis is accurate and thorough.

Q19. Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?

By clicking the Section Reviewed/Confirmed button you are confirming that all questions within the section have been reviewed and/or updated by the current user as of the current date. Continue?

OK Cancel

Section Reviewed/Confirmed

Reviewed By: John Doe Review Date: Tue Sep 09 14:41:02 EDT

Additional Information (Click Next to save any changes at this page)

Documents

< Back Next >

Security Risk Assessment Tool

Application Version: 3.6

Detailed Report

Doe Clinic

09-09-2025

DISCLAIMER

The Security Risk Assessment Tool at <http://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 organizations. 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 Health Information Privacy website at: <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 7/29/2025

Q20. How do you evaluate the effectiveness of your security safeguards, including physical safeguards?

Answer	We do not have a formal process to evaluate the effectiveness of our security safeguards.		
Education	Consider conducting technical and non-technical evaluations of security policies and procedures. This should be done periodically and in response to changes in the security environment.		
References	Compliance	Username	Audit Date
HIPAA: §164.308(a)(8) NIST CSF: ID.AM, GV.OC, ID.RA, PR.PS, DE.AE, DE.CM, RS.MI, ID.IM, RC.MI HPH CPG: 19 HICP: N/A	Required	John Doe	Tue Sep 09 14:36:15 EDT 2025
Reviewed Date	09-09-2025		
Reviewed By	John Doe		

Updated Report Covers

The Detailed Report PDF now includes any Section Reviewed/Confirmed details, including the approver's username and “reviewed-by” date, and any Additional Information that was saved.

The approval or confirmation details can be part of your completed SRA.

Report covers also include updated disclaimers.

Revised scoring terminology

SRA Tool 3.6 has “medium” changed to “moderate” to match the NIST Risk Management Framework scoring scale.

“Moderate” is now present in the SRA Tool 3.6 application, reports, and Workbook version.

This change came from a user suggestion during the 2024 SRA Tool webinar.

Section 1: SRA Basics

Vulnerabilities selected on the previous screen are shown below. Each vulnerability has threats associated with it. Consider each [threat](#) and how it might relate to your practice. Rate each for the likelihood of the threat occurring and the impact on your organization should it occur.

✓ Inadequate risk awareness or failure to identify new weaknesses

Likelihood: L M H Impact: L M H

Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches

Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)

Risk Report

Understand your security risk assessment by reviewing the matrix below. Click within each section to view your areas of review and corrective action plans.

Risk Breakdown

2 5 3 6

Risk Assessment Rating Key

Risk Assessment Rating Key		Impact		
		Acceptable little to no effect	Tolerable moderate effect	Intolerable critical effect
Likelihood	Improbable risk unlikely to occur	Low	Moderate	High
	Possible risk likely to occur	Low	Moderate	Critical
	Probable risk will occur	Moderate	High	Critical

Vulnerabilities

Section 1: SRA Basics

Vulnerabilities & Threats

Inadequate risk awareness or failure to identify new weaknesses

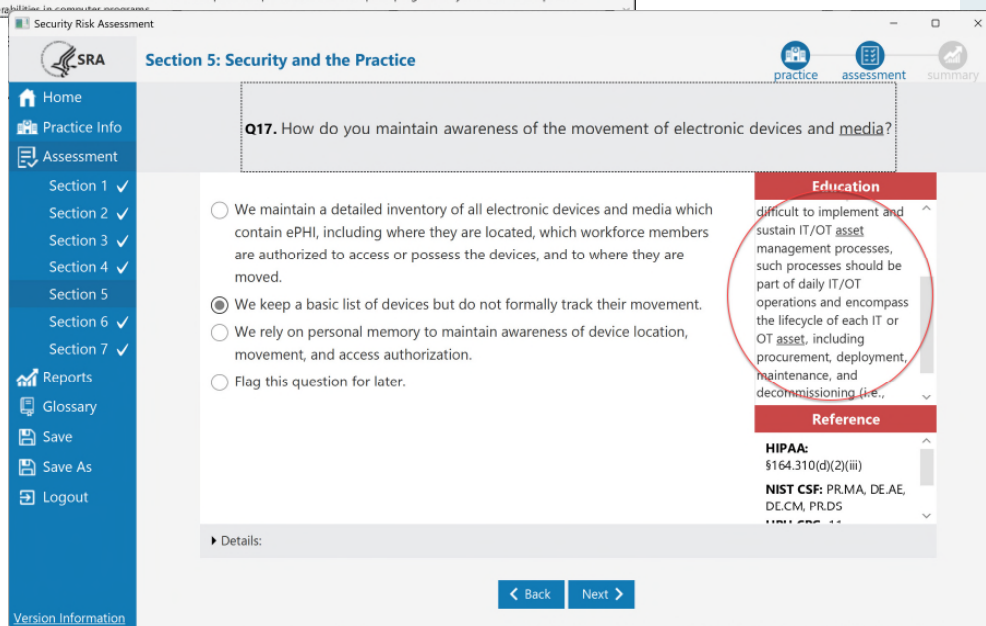
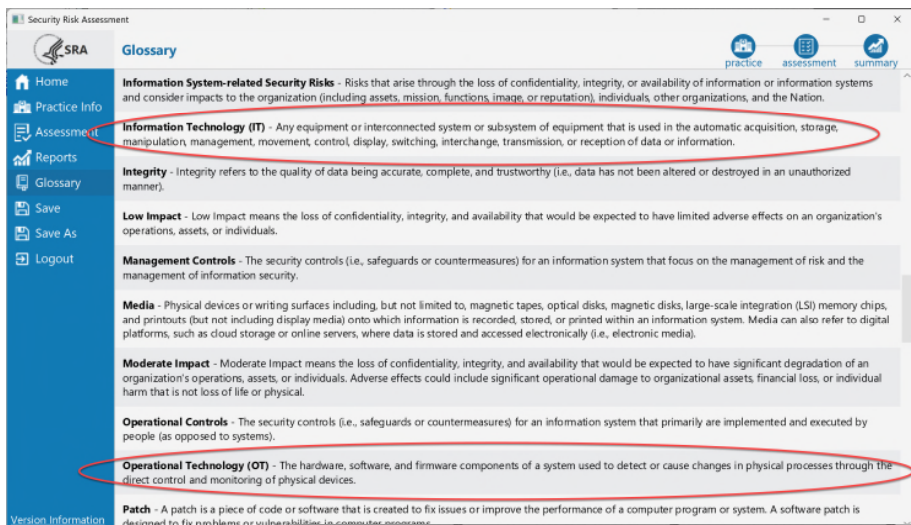
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches

Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)

High

Moderate

Back Next



New and Improved Content

SRA Tool 3.6 includes 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.

Examples include:

- Removal of one duplicate question
- Updating references to information technology (IT) to also include operational technology (OT)
- Changing “anti-virus” references to “malware protection”



Updated library files & Digital Cert

The SRA Tool 3.6 build includes refreshed library files to mitigate vulnerabilities in outdated components.

It is recommended that you uninstall your existing SRA Tool version when installing version 3.6.

Users can also review the installer file's digital certificate before installing the SRA Tool. The certificate helps confirm the authenticity and integrity of software installation file.

Steps for reviewing the digital cert are shown at left.

Conducting a Thorough Assessment



The HIPAA Security Rule's risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of the ePHI the organization creates, receives, maintains, or transmits.

- When responding to questions to identify and assess potential risks, organizations should consider how the questions apply throughout its entire enterprise.
- Organizations should take care that its responses reflect an accurate and thorough assessment of the questions presented and are not merely a clerical exercise to produce a report.
- Responding to questions without considering how the questions apply throughout the organization may result in a risk analysis that is not accurate and thorough as required by the HIPAA Security Rule.

Frequently Asked Questions

How do I upgrade to the latest version of the SRA Tool without starting over from scratch?

The installer is designed to overwrite the previous version of the tool without issue. Files created with previous versions of the tool will still work. However, if you continue working on older files, you may be missing out on content updates, including new assessment questions that appear in version 3.5 content.

How do I update the Audit Date displayed in the Detailed Report?

Audit Date reflects the last date a question was updated. The Audit Date will only be changed if the response is changed. If you've reviewed and updated an older SRA file, the date of review can be included in your file name or Date modified.

Is SRA Tool available for Apple or Mac computers?

No. The desktop application does is not supported on MacOS, Linux, or any operating system other than Windows. If you wish to use the SRA Tool on one of these systems, you might consider the SRA Tool Excel Workbook.

Does the SRA File or report need to be submitted anywhere?

Your SRA is for your own records. It may be required for an incentive program, but that is outside of the scope of the tool. SRA files are not submitted to ASTP/ONC or OCR.

Questions From Chat

Risk Assessment

SRA

Section 1: SRA Basics

practice assessment summary

Home

Practice Info

Assessment

Section 1

Section 2 ✓

Section 3 ✓

Section 4 ✓

Section 5 ✓

Section 6 ✓

Section 7 ✓

Reports

Glossary

Save

Save As

Logout

Version Information

Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?

☐ Written and verbal communication as well as coordinated corrective action planning.

☒ Written communication only.

☐ Verbal communication only.

☐ We do not communicate risk assessment results to workforce members.

☐ Flag this question for later.

Education

Written results of your SRA should be communicated to the personnel responsible for responding to identified threats and vulnerabilities but also consider involving the personnel responsible for responding to identified threats and vulnerabilities in the creation of corrective action plans.

Reference

HIPAA: §164.308(a)(1)(ii)(B)

NIST CSF: ID.RA, ID.RM, RS.MI

HICP: N/A

Details:

< Back

Next >

Contact Us

Contact the SRA Tool Helpdesk:

Email: SRAHelpDesk@Altarum.org

Submit SRA Tool Questions via the [HealthIT Feedback Form](#)

Additional Information & Resources

- Visit [HealtIT.gov](https://www.healthit.gov) and the [SRA Tool Download page](#)
- [SRA Tool User Guide](#) on the SRA Tool Download Page
- [Guide to Privacy and Security of Electronic Health Information](#)
- [HealthIT Privacy and Security Resources for Providers](#)

Follow @HHS_TechPolicy on Twitter for updates on the SRA Tool