



The Office of the National Coordinator for  
Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

**OFFICE FOR CIVIL RIGHTS**

# SECURITY RISK ASSESSMENT TOOL | V3.01

Presenters: Lisa Steffey & Ryan Callahan  
Center for Connected Health | Altarum



# Agenda



- Review the Challenge and Solution
- Highlights of the SRA Tool
  - Overview of Functionality
  - Recent Improvements
  - Benefits of using the SRA Tool
- Continuous Improvement & Future Enhancements
- Questions & feedback

## Challenge

The healthcare industry constantly faces evolving cybersecurity threats and smaller healthcare providers often have limited time and resources to defend against the growing number of security risks.

The healthcare industry needs a Security Risk Assessment (SRA) tool that is easy to use and can help small practices evaluate their security posture against increasingly sophisticated security attacks.



## Solution

ONC engaged Altarum to design an improved version of the SRA Tool with a wizard-based workflow, updated layout, and an enhanced user experience that can assist users with their risk analysis process.

The new SRA Tool has over 56,645 downloads in the past year.

# Arriving at the Solution



To better support the SRA user community and enhance the current tool, **True Intent Usability Testing** was conducted.

From the usability testing report, the following requirements were identified and a development plan created to:

- Revise the core content language by decoupling the questions from the legislative verbiage
- Improve the asset and BAA/vendor tracking features
- Add components to address applicable threats and vulnerabilities through a guided risk framework
- Improve the workflow by creating a modular approach, focusing on ease of use and time to complete the SRA
- Introduce branching logic to cut out unnecessary questions
- Enhance the usability and user experience with a more modern interface

# Overview of Functionality

- The SRA Tool guides organizations through a self-paced security risk assessment covering administrative, physical, and technical safeguards.
- The SRA Tool 3.0 contains:
  - New User Interface
  - Improved Asset tracking feature
  - Expanded Vendor tracking feature
  - Revised Assessment questionnaire content
  - Guided Risk Framework
  - Threats & Vulnerability Rating
  - Section Summary Reports
  - Detailed SRA Report and Risk Report



The screenshot shows the SRA Tool 3.0 user interface. At the top left is the SRA logo. To its right is a "Welcome!" message. On the far right, there are three navigation icons labeled "practice", "assessment", and "summary". A blue sidebar on the left contains a menu with the following items: Home, Practice Info, Assessment, Summary, Save, and Logout. The main content area features a header image of a stethoscope on a desk with charts. Below the image is the text "What's a Security Risk Assessment?" followed by a paragraph explaining that a security risk analysis is the foundation for protecting ePHI. Below this is a section titled "The SRA tool has 3 core steps:" with three numbered steps: Step 1: Enter your practice information, Step 2: Answer the assessment questions, and Step 3: Review your final risk report. To the right of the steps is a diagram of three red circles connected by lines, each containing an icon representing a step. At the bottom right of the main content area is a blue "Next >" button.



# Content 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
- NIST Cybersecurity Framework

# Improved User Interface

Navigation Panel

Section Indicator

Summary Reports

**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  
Summary  
Save  
Logout

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.

< Back   Next >

**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.

**Reference**

For additional information, see Security Rule 45 CFR §164.316(a)

← Question

← Education & Dynamic Feedback

← Related Standard



# Core Assessment Areas

- Asset tracking
- Business Associate Agreements/Vendor tracking
- Data security (i.e., encryption)
- Hardware security (i.e. proxy servers, firewalls, etc.)
- Facility security (i.e., locked access points)
- Access control (i.e., unique ID's and passwords for all team members)
- Personnel security
- Third parties
- Contingency planning (i.e., data backups)
- Policies, Procedures, and Documentation

# Enhanced Asset Tracking



## Available Fields:

- Asset Type
- Asset Status – active, inactive
- ePHI Access – does it access PHI?
- Disposal Status – if inactive, has it been properly wiped/disposed
- Disposal Date – date asset was disposed
- Asset Encryption – type of encryption protection of data
- Asset Assignment – who is responsible for this asset?
- Asset ID – asset tag or internal identifier

The screenshot shows the 'Add Asset' form in the SRA Practice Assets interface. The form is a modal window with a blue header and a white body. It contains several fields:

- Asset Type:** A dropdown menu with 'Laptop' selected.
- Asset Status:** A dropdown menu with 'Inactive [Storage]' selected.
- ePHI Access:** A dropdown menu with 'Receives and tran...' selected.
- Disposal Status:** A dropdown menu with 'Not Disposed' selected.
- Disposal Date:** A text input field with a calendar icon.
- Asset Encryption:** A dropdown menu with 'Full disk encryption' selected.
- Asset Assignment:** A text input field with 'John Appleseed' entered.
- Asset ID:** A text input field with 'CID-22120' entered.
- Comments:** A large text area for additional notes.
- Add:** A blue button at the bottom right of the form.

At the bottom of the form, there are two navigation buttons: '< Back' and 'Next >'. The background shows the SRA Practice Assets dashboard with a sidebar on the left and a main content area on the right.

# Expanded Vendor/BAA Tracking



**Practice Vendor Add Vendor**

Vendor Name: Lab Testing llc.

Service Type Provided: laboratory services

Vendor Address: 110 Fifth St.

City, State, Zip: Ann Arbor MI 48103

Phone, Fax: (xxx)-xxx-xxxx (xxx)-xxx-xxxx

Contact Name/Title:

Contact Email:

+ Second Contact

Have [satisfactory assurances](#) been obtained for this vendor?  Yes  No

Have additional risks been assessed for this vendor?  Yes  No

Add

## Available Fields:

- Vendor Name
- Service Type Provided
- Vendor Address
- City, State, Zip
- Phone, Fax
- Contact Name/Title
- Contact Email
- Satisfactory Assurances – contract that PHI will be protected
- Additional Risks -
- + Second Contact – add another contact for the vendor

# New Practice Documentation Feature

**Documentation**

practice assessment summary

Home  
Practice Info  
Assets  
Vendors  
Documents  
Assessment  
Summary  
Save  
Logout

Add [additional documentation](#) to your SRA.  
Add documents, action item lists, references, remediation plans, or plan of action milestones relevant to your security risk assessment.

**Add a Document**

Manage Documents	Document Name	Section	Added By	Date Added
No content in table				

< Back   Next >



The Documentation screen allows users to link to supporting documentation for the assessment.

Documents added to an SRA are links to documents stored locally or on a local network to demonstrate accuracy and thoroughness of your responses.

Documents that have been added from the section summary screens also display here.

# New Threats & Vulnerabilities Section



The screenshot displays the 'Section 1: SRA Basics' assessment interface. The top navigation bar includes 'practice', 'assessment', and 'summary' icons. A left sidebar contains navigation links: Home, Practice Info, Assessment (with sub-links for Section 1 through Section 7), Summary, Save, and Logout. The main content area features the instruction: 'Select the [vulnerabilities](#) that apply to your practice from the list below.' Below this, five vulnerability items are listed with checkboxes:

- Inadequate risk awareness or failure to identify new weaknesses
- Failure to remediate known risk(s)
- Failure to meet minimum regulatory requirements and security standards
- Inadequate Asset Tracking
- Unspecified workforce security responsibilities

At the bottom of the interface, there are two buttons: '< Back' and 'Next >'.

The Vulnerability selection screen is presented after each assessment section.

Users are asked to select from a list of vulnerabilities that may be applicable to their practice.

# Rating Threats & Vulnerabilities



**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  
Summary  
Save  
Logout

Please rate the likelihood and impact on your practice of each potential [threat](#).

✓ Inadequate risk awareness or failure to identify new weaknesses

	Likelihood			Impact		
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches	L	M	H	L	M	H
Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)	L	M	H	L	M	H
Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or destruction from animals/insects	L	M	H	L	M	H
Man-Made threat(s) such as insider carelessness, theft/vandalism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals	L	M	H	L	M	H
Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof,	L	M	H	L	M	H

Following the selection of applicable vulnerabilities, the Threat Rating screen is presented.

A Guided Risk Framework allows users to review a list of related threats and rate each one in terms of likelihood and impact should they occur.

# Modular Workflow with Section Summaries



**SRA**

**Section 1: Complete!**

practice assessment summary

Home  
Practice Info  
Assessment  
Section 1 ✓  
Section 2  
Section 3  
Section 4  
Section 5  
Section 6  
Section 7  
Summary  
Save  
Logout

Congratulations you've completed Section 1, on SRA Basics. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

89% 11%

**Areas of Success**

- ▶ **Q1.** Has your practice completed a security risk assessment (SRA) before?
- ▶ **Q2.** Do you review and update your SRA?
- ▶ **Q3.** How often do you review and update your SRA?
- ▼ **Q6.** What do you include in your SRA documentation?  
**Your Answer:** Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity. We develop corrective action plans as needed to mitigate identified security

**Areas for Review**

- ▼ **Q4.** Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?  
**Your 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.

The Section Summary shows each of the questions answered, responses, and education content.

Questions are divided into **Areas of Success** and **Areas for Review**.

Questions sorted into Areas of Success are those which represent the lowest level of risk.

Areas for Review represent responses that could use improvement.

# SRA Reports



Risk Score – shows Areas for Review as a percentage of the total questions answered.

Areas for Review – sum of questions answered sorted into Areas for Review.

Vulnerabilities – sum of vulnerabilities selected as applicable to the practice.

The bottom portion of this screen is the Risk Score broken down by section.

# Improved Reports



**Risk Report**

practice assessment summary

Home Practice Info Assessment Summary Risk Report Detailed Report Save Logout

**Risk Breakdown**

3 42 19 35

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

The Risk Report identifies all areas of risk collected in each section of the assessment.

Each vulnerability selected is shown here along with each response sorted into Areas for Review.

Risk Breakdown – shows a sum of threat ratings in each risk category.

Risk Assessment Rating Key – shows how likelihood and impact ratings combine to show the risk level.



# What are benefits of the SRA Tool?

- Intuitive user interface
- Self-paced with a modular workflow
- Custom assessment logic
- Progress tracker
- Dynamic feedback on each question
- Includes guided risk ratings for potential threats & vulnerabilities
- Offers detailed reports focused on areas of risk so users can target specific areas for remediation
- Provides a framework for conducting a thorough risk assessment
- Offers a structured means to assist entities with the HIPAA Security Rule's risk assessment requirement



# What have we learned from users?

After the initial launch of the revised SRA Tool in the fall of 2018 we conducted several [webinar trainings](#).

User feedback and target areas for continued improvement:

- Access to printable reports
- Access to view SRA results in Excel
- Access to review and update previous year's assessments
- Functionality that allows skipping sections or questions
- Easy access to attach supporting documentation in more areas of the tool
- View references to the NIST Cyber Security Framework



# Continuous Improvement & Upcoming Enhancements

## 3.1 (upcoming release)

- Highlight missed threat and vulnerability ratings
- Mechanism to select multiple and “delete all” assets and vendors
- Adding NIST Cybersecurity Framework references to each question
- Excel export of Detailed Report
- “In Process” reporting functionality, question flagging (skip question)

# Questions and Feedback

Submit Questions to [HealthIT Feedback Form](#)

Or contact the SRA Tool Helpdesk:

Email: [SRAHelpDesk@Altarum.org](mailto:SRAHelpDesk@Altarum.org)

Phone: 734-302-4717

Reference the [SRA Tool User Guide](#)

Watch the recorded [webinar trainings](#)

Review the SRA Tool training [slide deck](#)





## What's Next?

We are compiling the additional feedback we received in July and August of this year and will work with ONC and OCR to prioritize additional fixes and enhancements.