ALTARUM

SOLUTIONS TO ADVANCE HEALTH

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

Content Sources

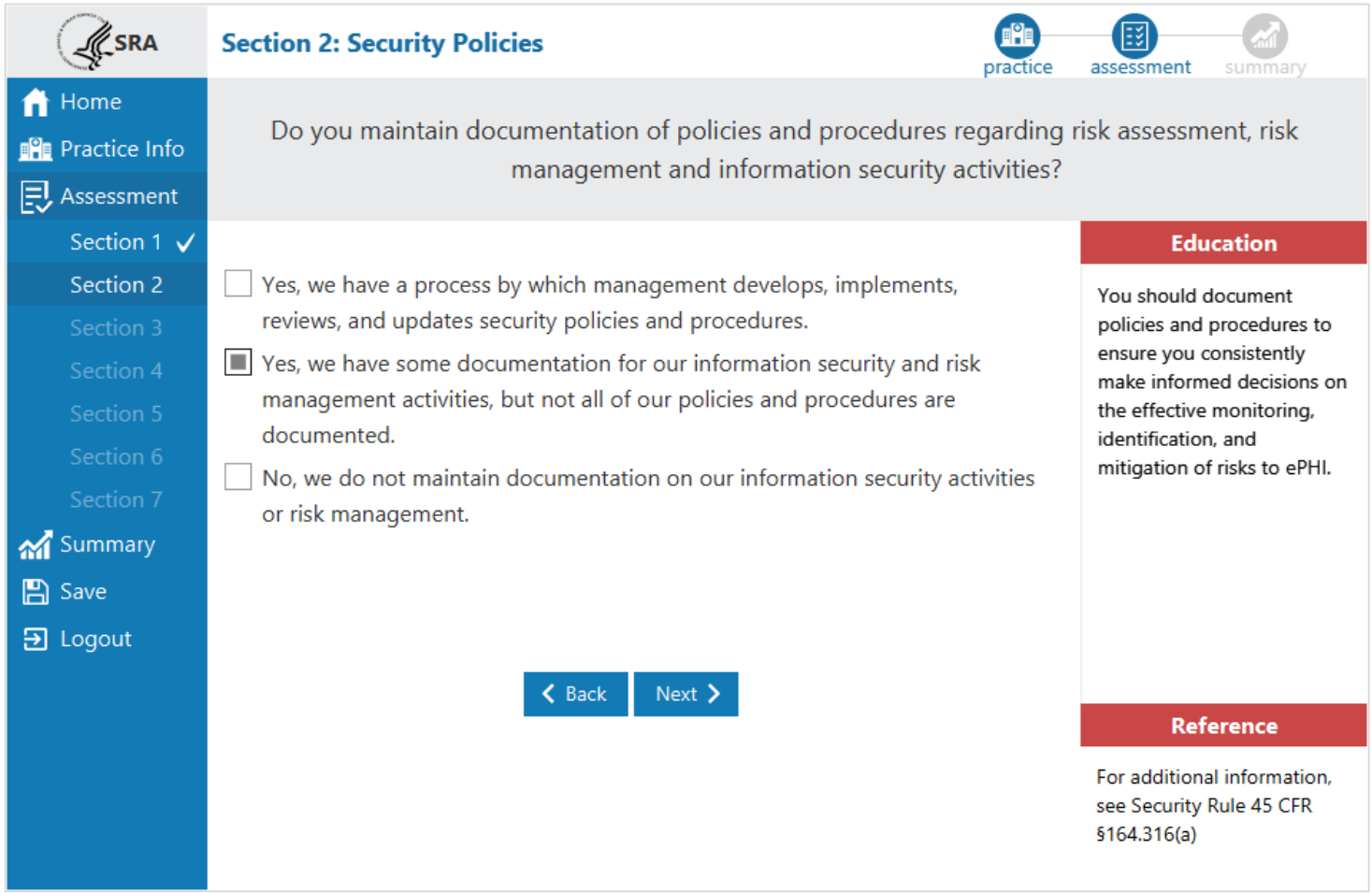
- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication 800-66
- NIST Special Publication [Guide to Implementing FISMA Security Controls] 800-53
- NIST Special Publication [Guide to Assessing FISMA Controls] 800-53A
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- NIST Cybersecurity Framework

Improved User Interface

Navigation Panel

Section Indicator

Summary Reports



Question

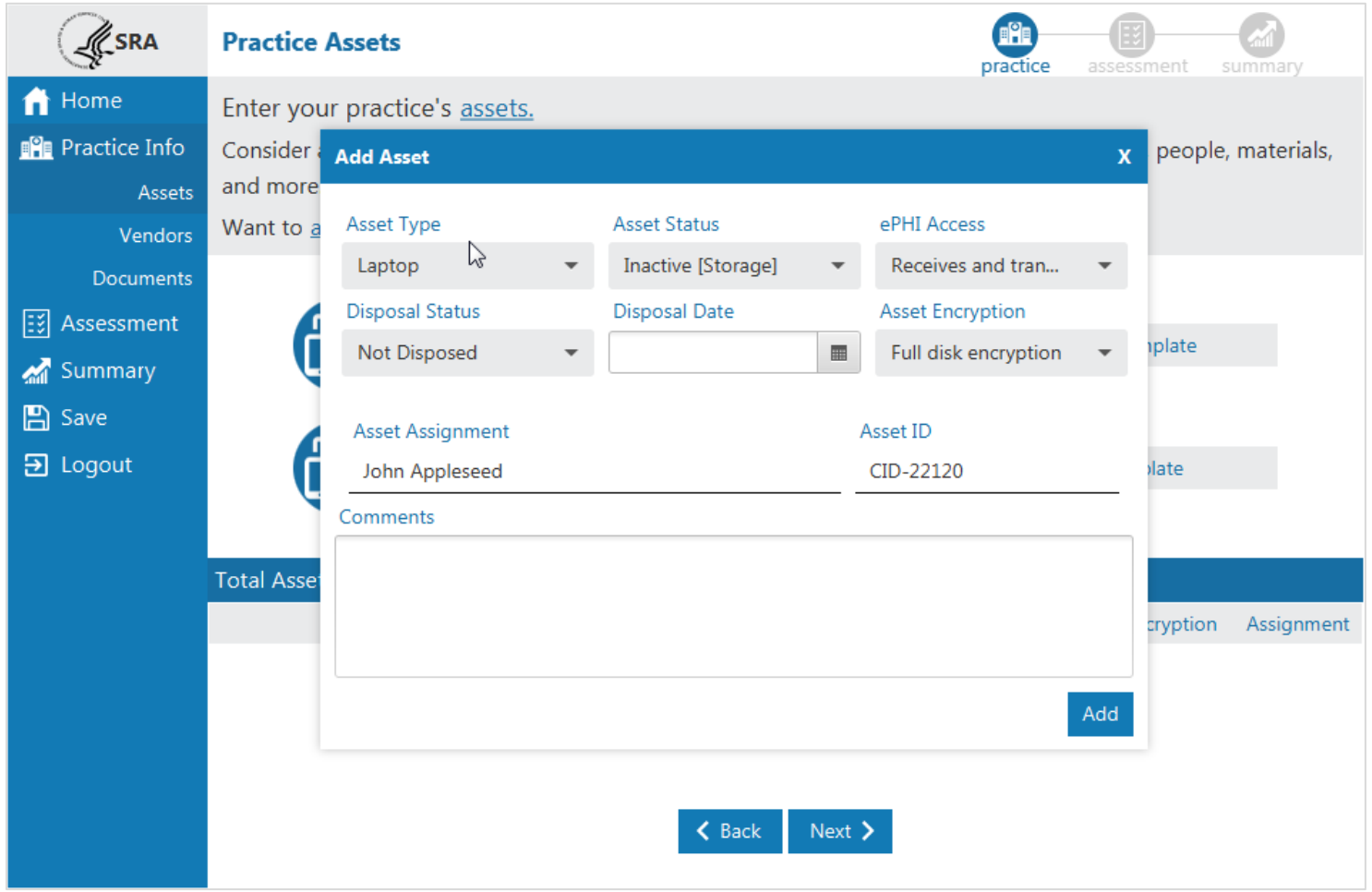
Education & Dynamic Feedback

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

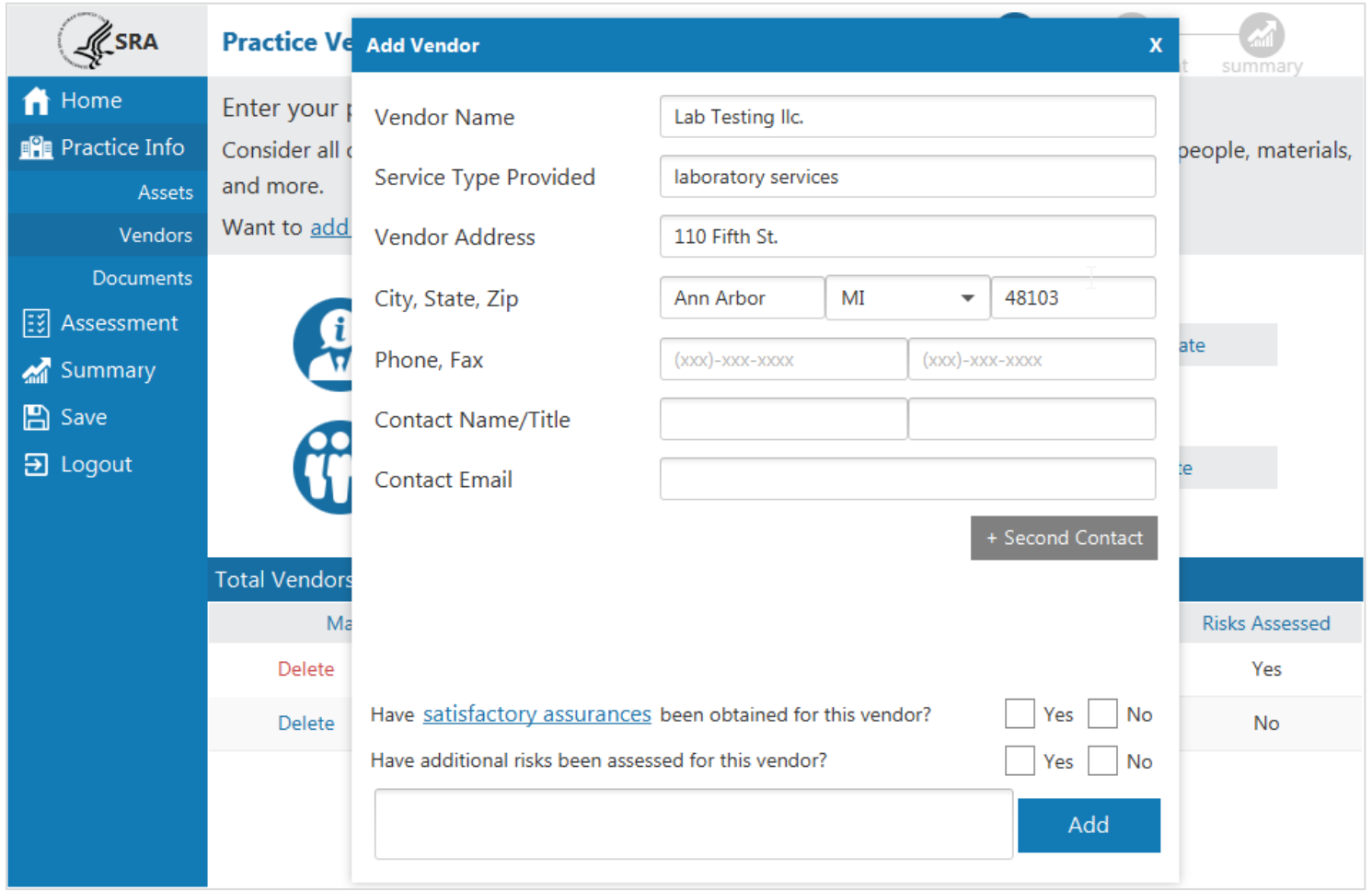
Enhanced Asset Tracking



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

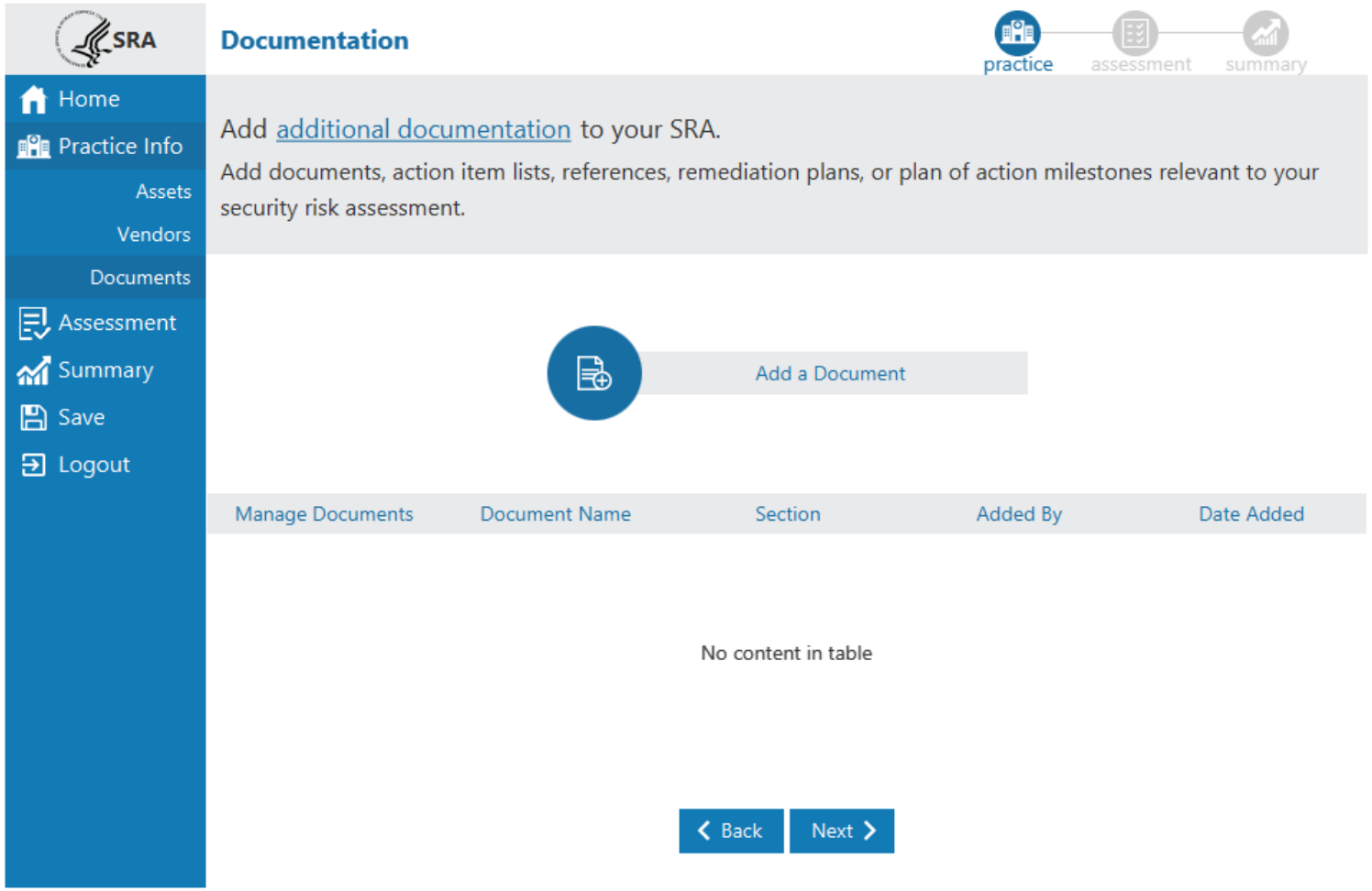
Expanded Vendor/BAA Tracking



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

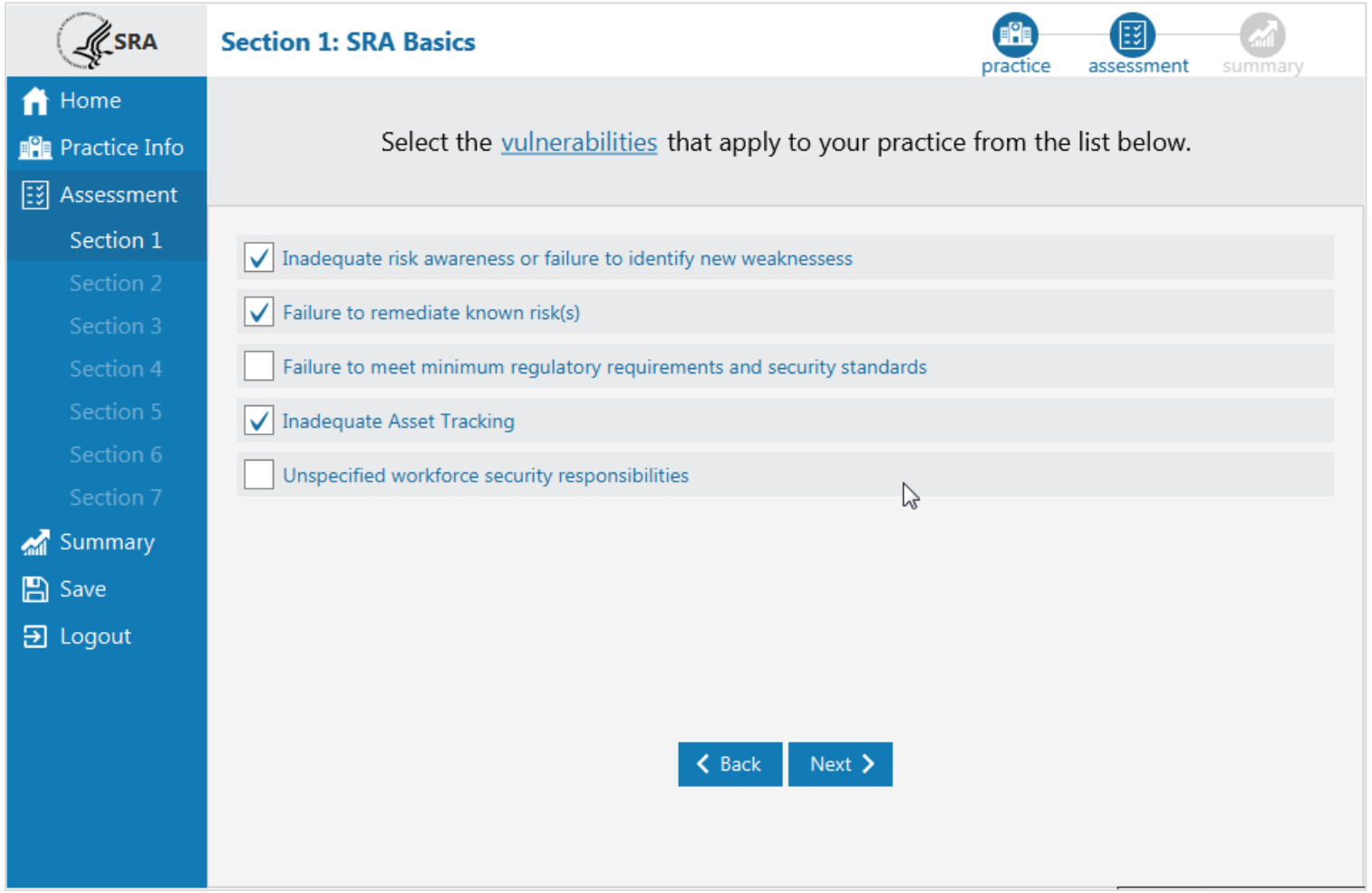


The Documentation screen allows users to link to supporting documentation for the assessment.

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.

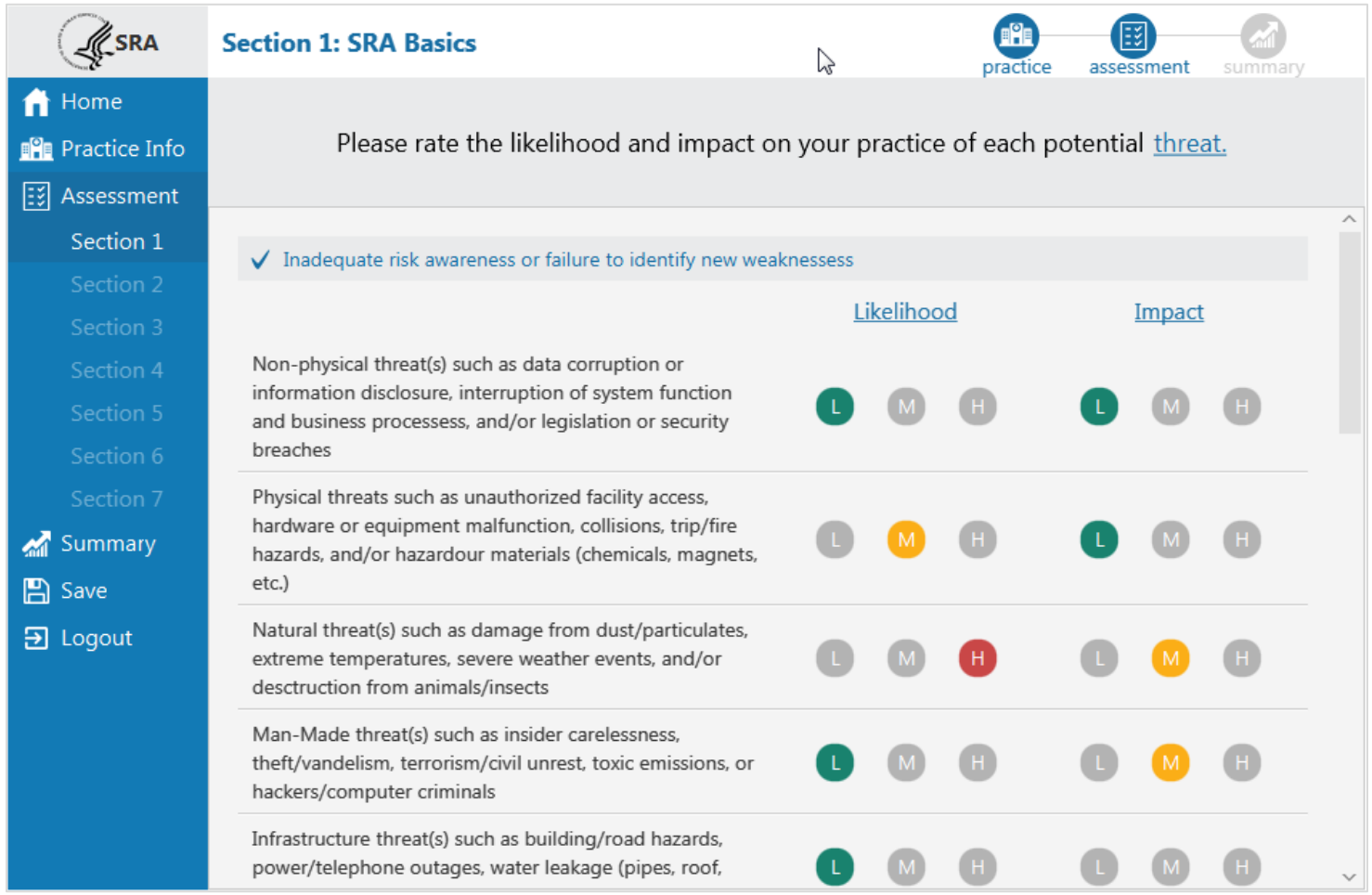
New Threats & Vulnerabilities Section



The 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.

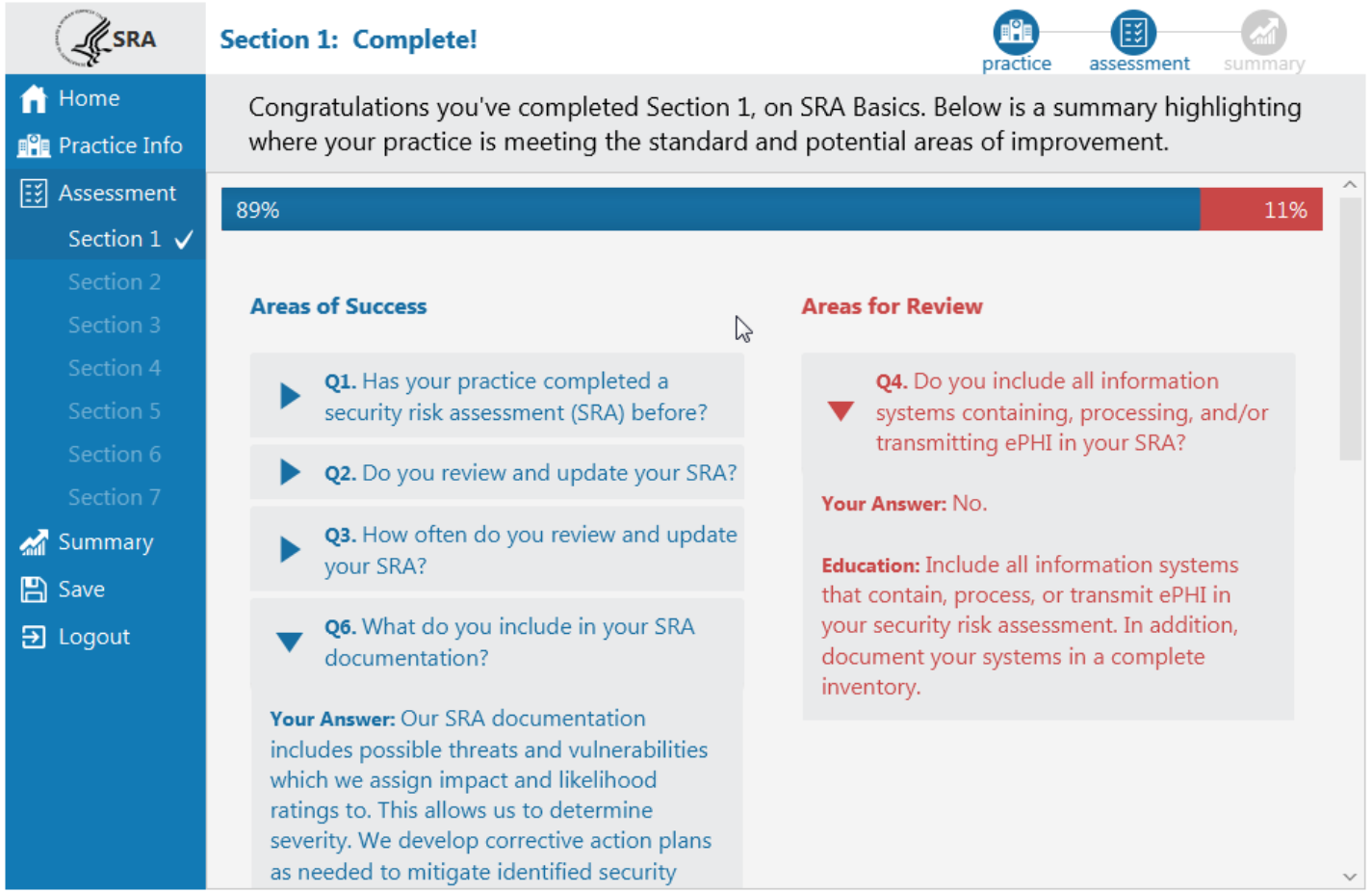
Rating Threats & Vulnerabilities



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



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

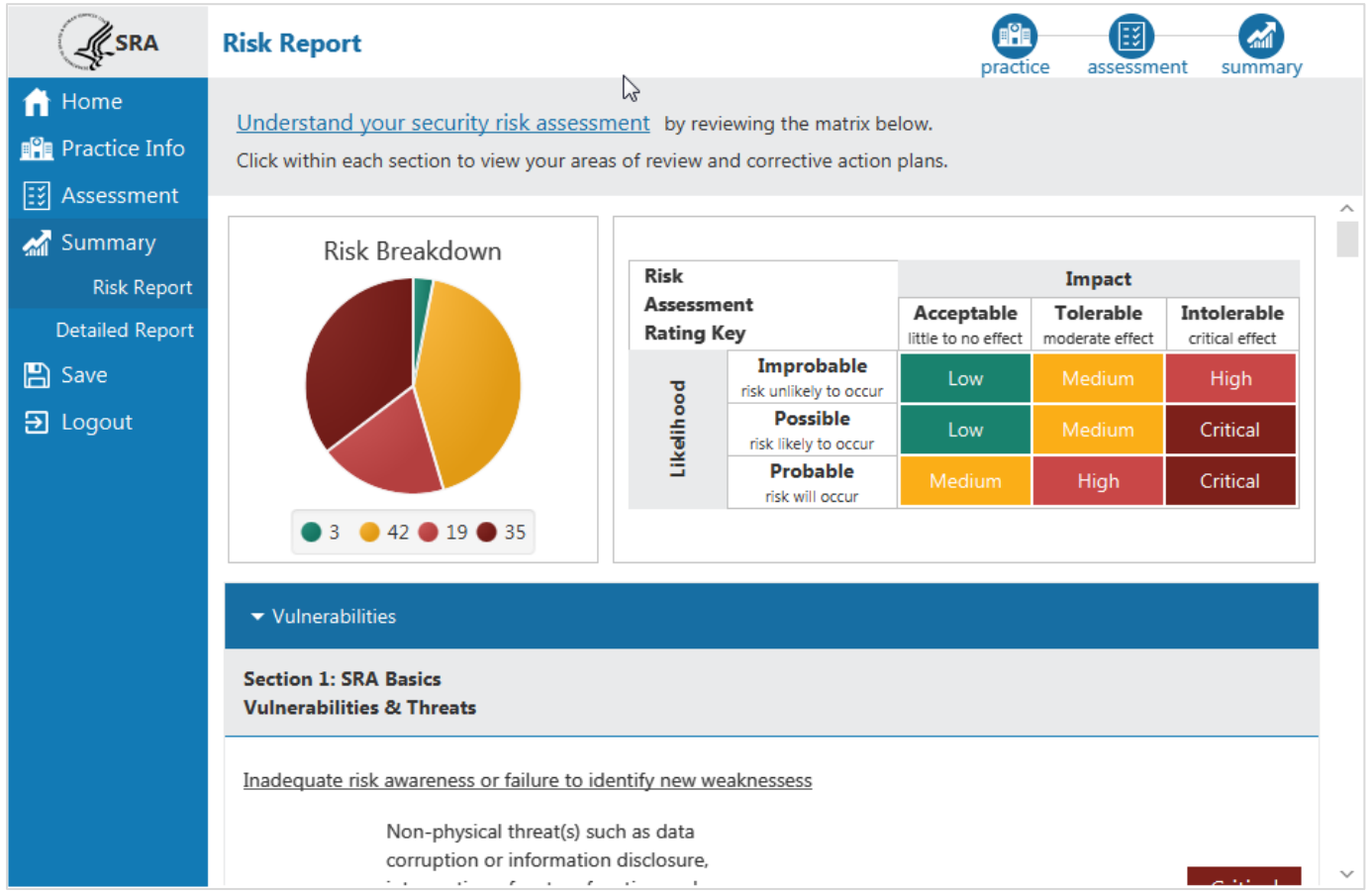
Risk Score – shows Areas for Review as a percentage of the total questions answered.

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



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

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 enhncements.