ACET

AUTOMATED CYBERSECURITY EVALUATION TOOLBOX

National Credit Union Administration

USER MANUAL

Automated Cybersecurity Evaluation Toolbox(ACET), Version 10.2.

User Manual

April 2021

This product was developed by the National Credit Union Administration (NCUA).

Table of Contents

Introduction to ACET

This section will help the user better understand the Automated Cybersecurity Evaluation Toolbox (ACET), its background, and purposes.

Introduction

The Automated Cybersecurity Evaluation Toolbox (ACET) provides the following:

1. A framework for analyzing cybersecurity vulnerabilities associated with an organization's overall industrial control system (ICS) and information technology (IT) architecture;

2. A consistent and technically sound methodology to identify, analyze, and communicate to security professionals the various vulnerabilities and consequences that may be exploited by cyber means;

3. The means for the user to document a process for identifying cybersecurity vulnerabilities; and

4. Suggested methods to evaluate options for improvement based on existing Standards and recommended practices.

Background

The Automated Cybersecurity Examination Tool (ACET) Maturity Assessment is an assessment of a Credit Union's Inherent Risk and Cybersecurity Maturity. The ACET provides the NCUA with a repeatable, measurable and transparent process for assessing the level of cyber preparedness across federally insured institutions.

The ACET incorporates appropriate standards and practices established for financial institutions. It also aligns with the Cybersecurity Assessment Tool developed by the FFIEC for voluntary use by banks and credit unions.

The ACET consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components, and individual Declarative Statements across five maturity levels.

ACET is a web-based tool that guides users through a step-by-step process to collect facility-specific information addressing topics such as hardware, software, administrative policies, and user obligations. It then compares that information to relevant security Standards and regulations, assesses overall compliance, and provides appropriate recommendations for improving cybersecurity posture. The tool pulls its recommendations from a collection of the best available cybersecurity Standards, guidelines, and practices. Where appropriate, recommendations are linked to a set of actions that can be applied to enhance cybersecurity controls.

Objectives and Benefits

The primary objective of ACET is to reduce the risk of cyber attacks by identifying potential cybersecurity vulnerabilities within a system or an organization. ACET implements a simple, transparent process that can be used effectively by all sectors to perform an evaluation of any network. It offers the following benefits:

- Provides a repeatable and systematic approach for assessing the cybersecurity posture of a system, network, site, or facility.
- Provides a comprehensive evaluation and comparison to existing industry Standards and regulations.
- Combines the ICS and IT security knowledge and experience of many organizations.
- Assists in the identification of potential vulnerabilities in the network design and security policies.
- Provides guidelines for cybersecurity solutions and mitigations.
- Provides access to a centralized repository of cybersecurity requirements.
- Provides an opportunity for dialogue on security practices within the user's facility.

Limitations of this Tool

The tool has a component focus rather than a system focus. Therefore, network architecture analyses, including network hardware and software configuration analyses, will be limited to the extent that they are defined by programmatic and procedural requirements.

Most importantly, ACET is only one component of a comprehensive control system security program. A security program based on a ACET assessment alone must never be considered complete or adequate.

User Qualifications

ACET assessments cannot be completed effectively by any single individual. A cross-functional team consisting of representatives from multiple company areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to be able to fully and accurately answer all the questions provided by the ACET tool.

Disclaimer

"The analysis, data, and reports in ACET® are provided “as is” for informational purposes only. The NCUA does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

NCUA does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by NCUA.

The display of the NCUA official seal or other NCUA visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of NCUA. The NCUA seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by NCUA or the United States Government. Use of the NCUA seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against NCUA policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the ACET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the ACET Program."

System Basics

This section describes system requirements, installation instructions, and recommendations on how to go about preparing for the cybersecurity evaluation.

System Requirements Local Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing ACET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 6 GB free disk space
- 4 GB of RAM
- Microsoft Windows 10 or higher
- Microsoft .NET Framework 4.7 Runtime
- SQL Server 2012 Express LocalDB (included in ACET installation)
- IIS Express 8 (included in ACET installation)

Other Items of Note:

- For all platforms, it is recommended the user upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update web site to ensure the best compatibility and security.

- If the install must be made through physical media, a USB port will be required.

- If desired, HTML reports will need to be converted to PDF using an external utility.

- If the Microsoft .NET Framework 4.7 Runtime is not available on the user's computer, ACET will automatically install it, which can add several minutes to the installation time.

- Internet Explorer 11 and lower are not supported.

Installation Procedure

To install ACET follow the instructions below:

Double-click on the ACETStandAlone program.
The User Account Control dialogue will come up. Select “Yes”.

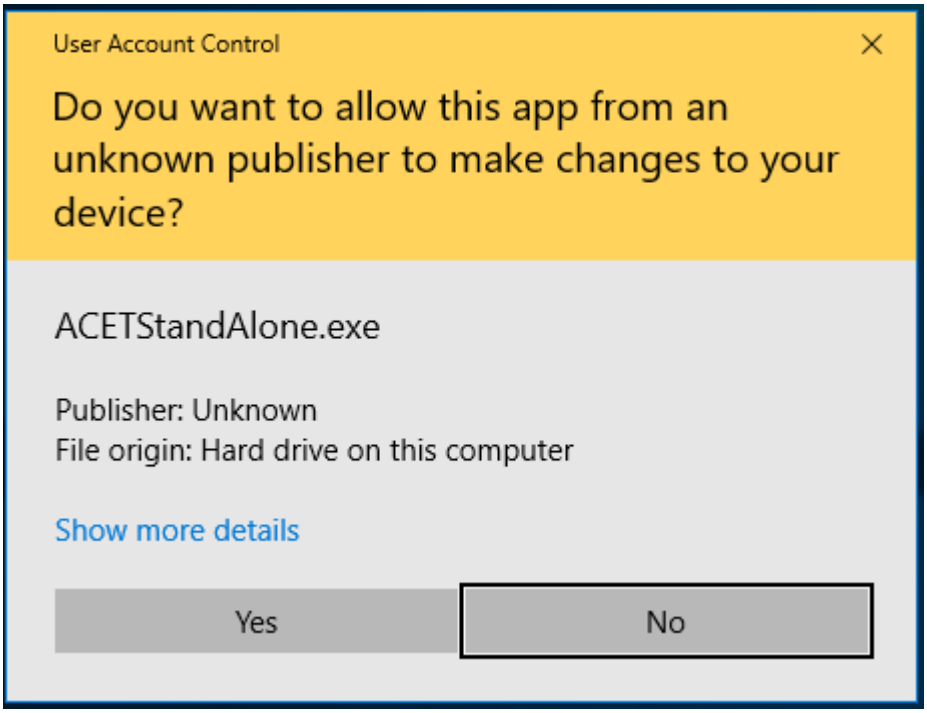


Figure: User Account Control box

A dialogue will open asking if you want to install ACET Desktop. Select “Yes”.

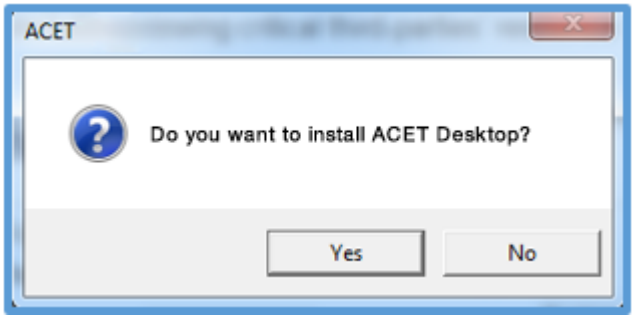


Figure: Install dialogue

The program will begin extracting.
After extracting an ACET Setup dialogue will open. Select the checkbox "I agree to the license terms and conditions" and then select “Install”.

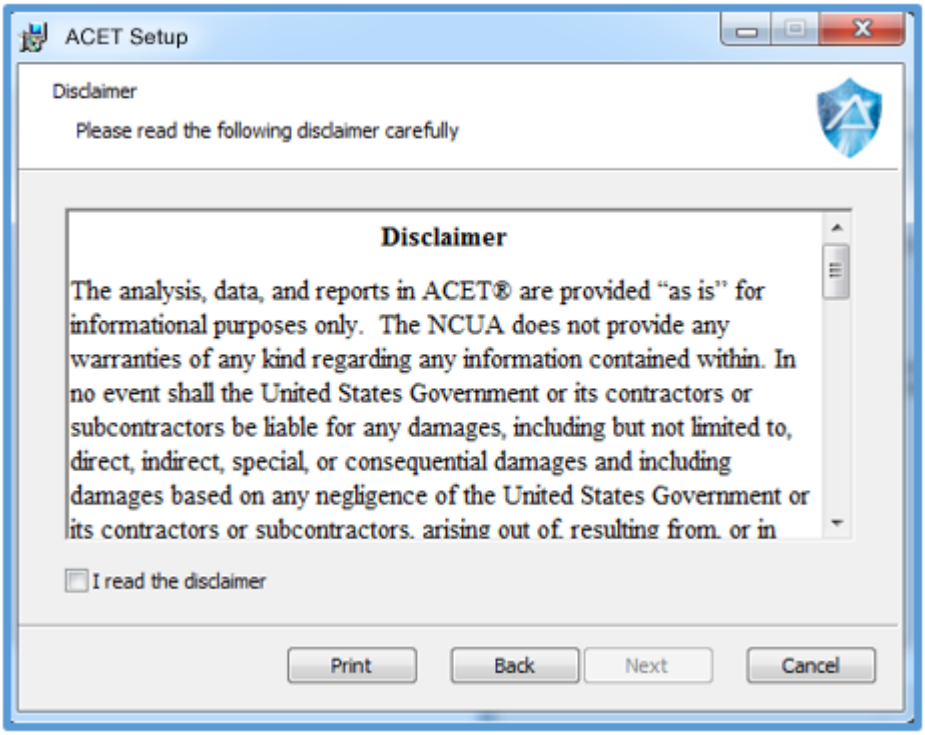


Figure: ACET Setup

ACET will begin to install. If the user doesn't have SQL Server 2012 Express, ACET will install it. The SQL Server 2012 Express Setup dialogue will open. Click "Next" and then select "Install".

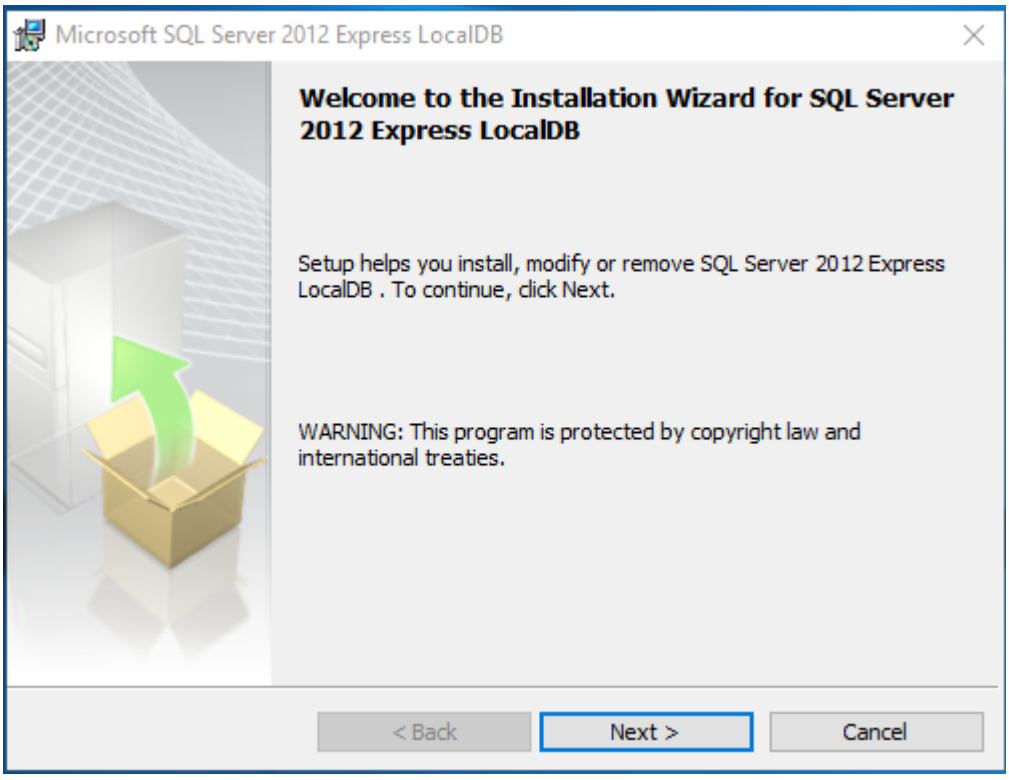


Figure: SQL Server Setup

If the user doesn't have IIS 10.0 Express, ACET will install it. The IIS 10.0 Express Setup dialogue will open. Click the check box to confirm that you "…accept the terms in the License Agreement", and then select "Install".

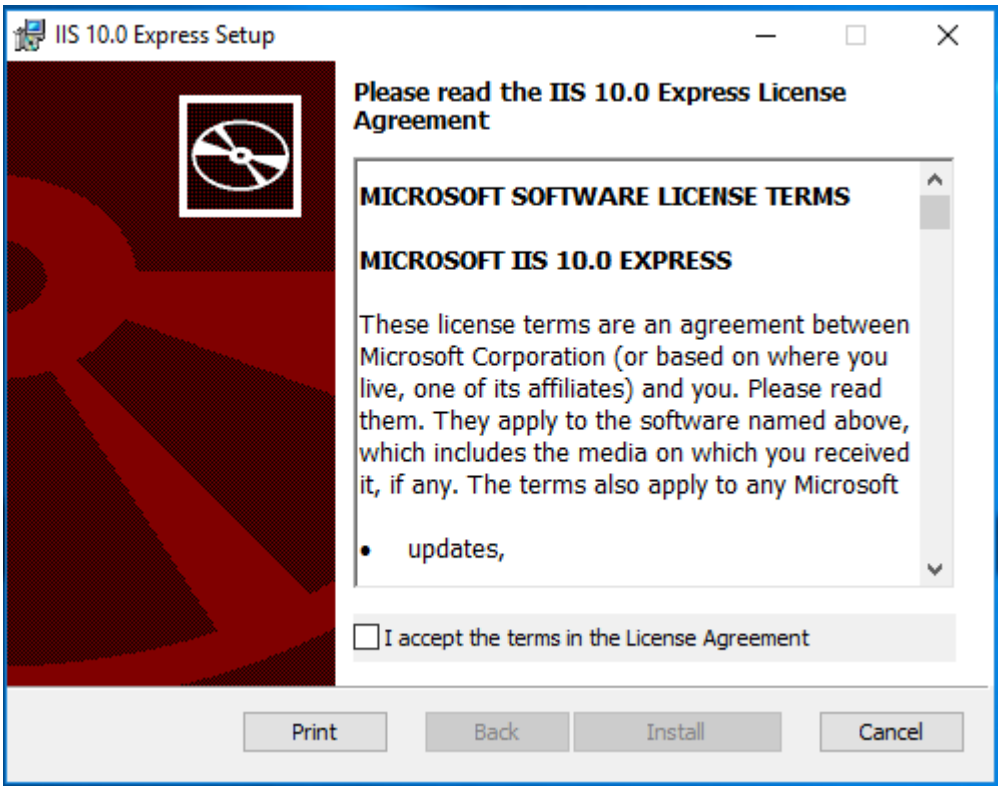


Figure: IIS Setup

IIS will install. Select “Finish” when it completes.
The ACET Setup Wizard will open to walk the user through the install process. Select “Next”.

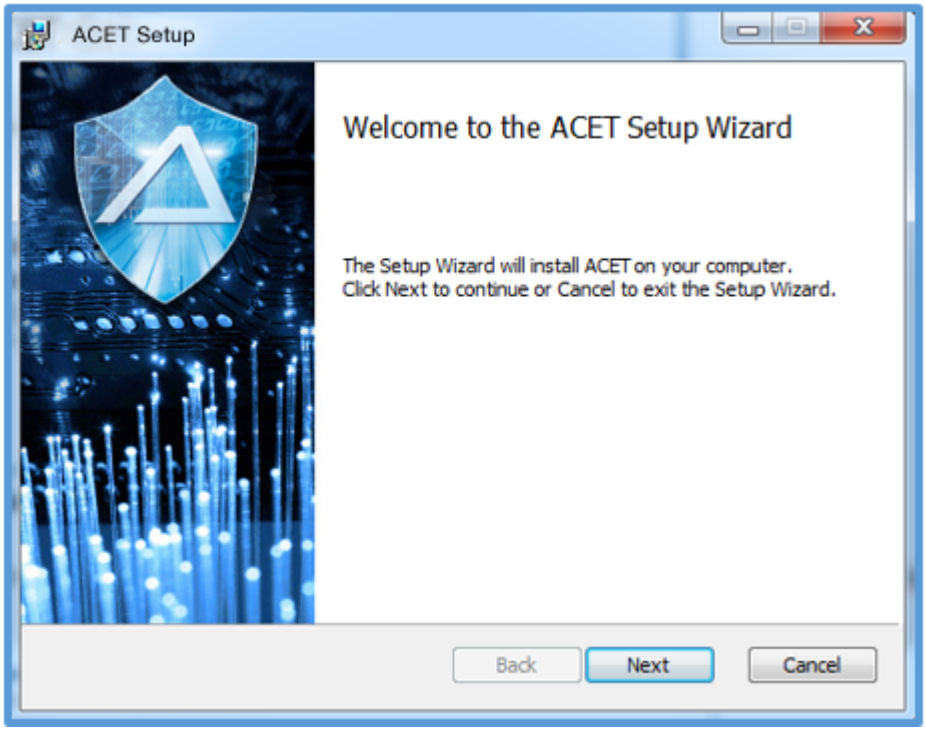


Figure: Setup Wizard

ACET will choose a default folder to install to. You can change this in the Destination Folder dialogue. Select “Next”.

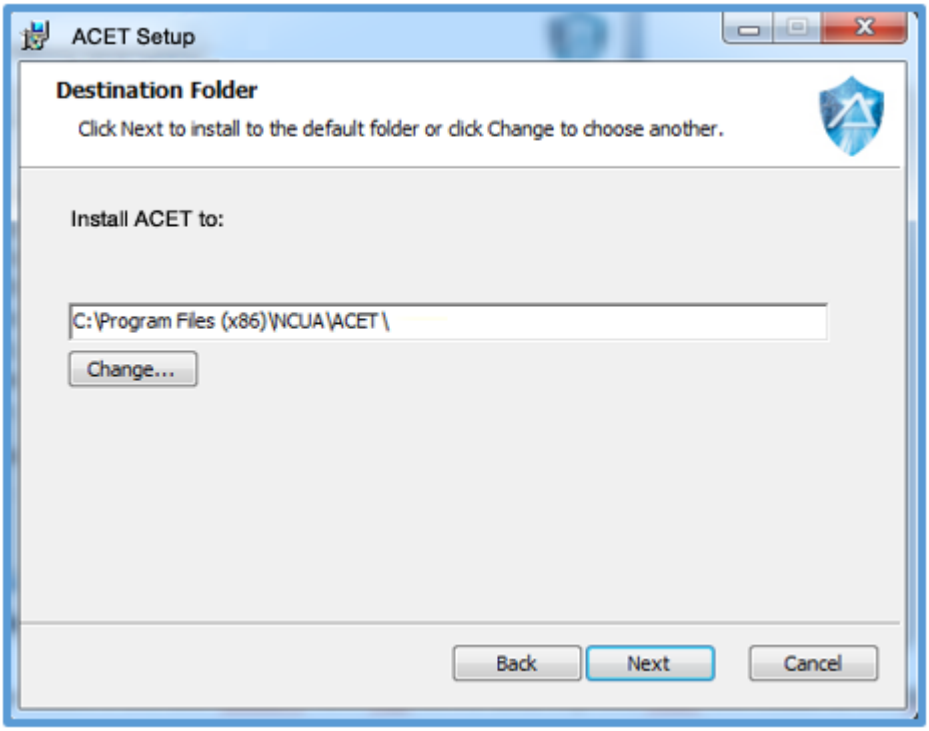


Figure: Destination Folder

The ACET Installer will show that it is ready to install, select “Install”.

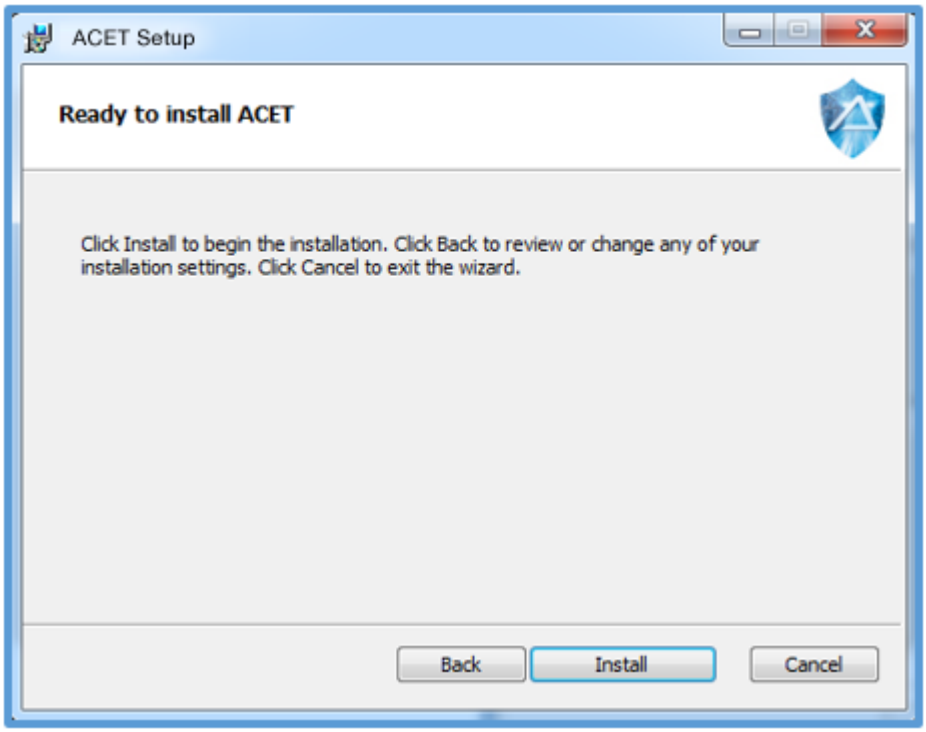


Figure: Ready to Install

ACET is installed. Make sure that the “Launch ACET when setup exists” box is checked and select “Finish”.
The user should see a setup successful dialogue, and have an option of how they want to open the app. For this example Edge was used.

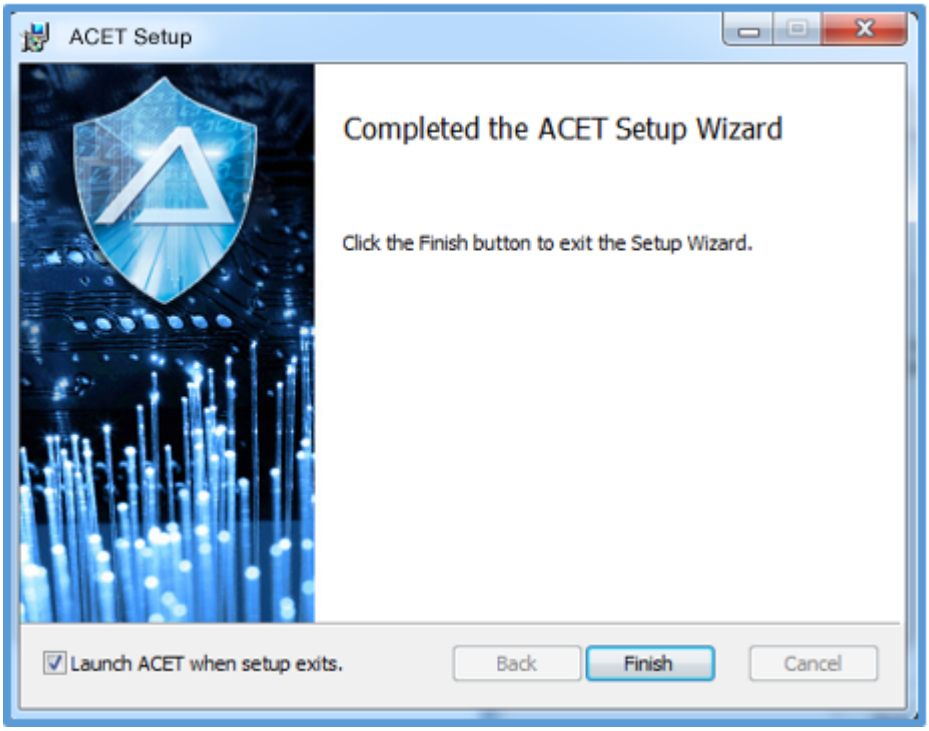


Figure: Setup Successful

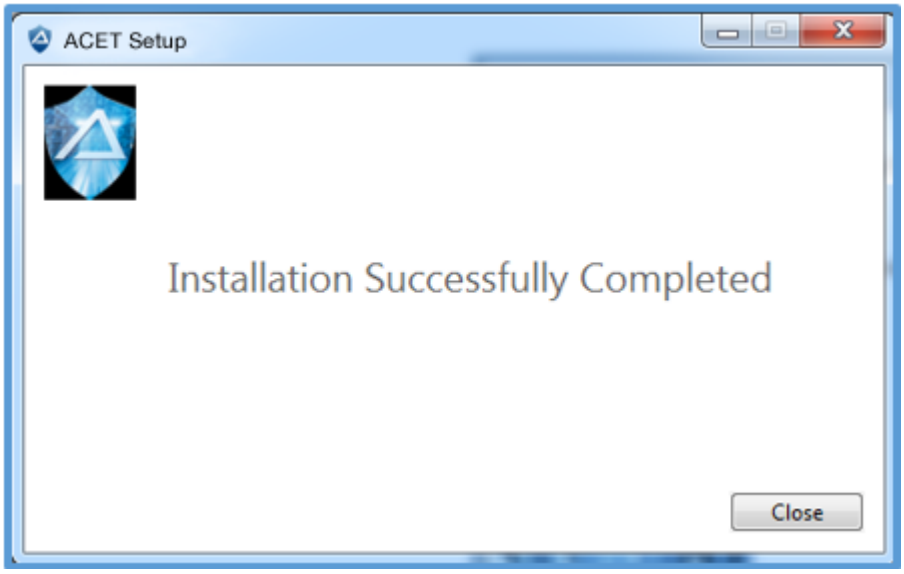


Figure: Installation Successful

After getting this message restart your machine.

The user has now has access to ACET under their Windows NT user name. The Local Installation ribbon is visible at the top of the screen. They can see their landing page with no assessments at this time.

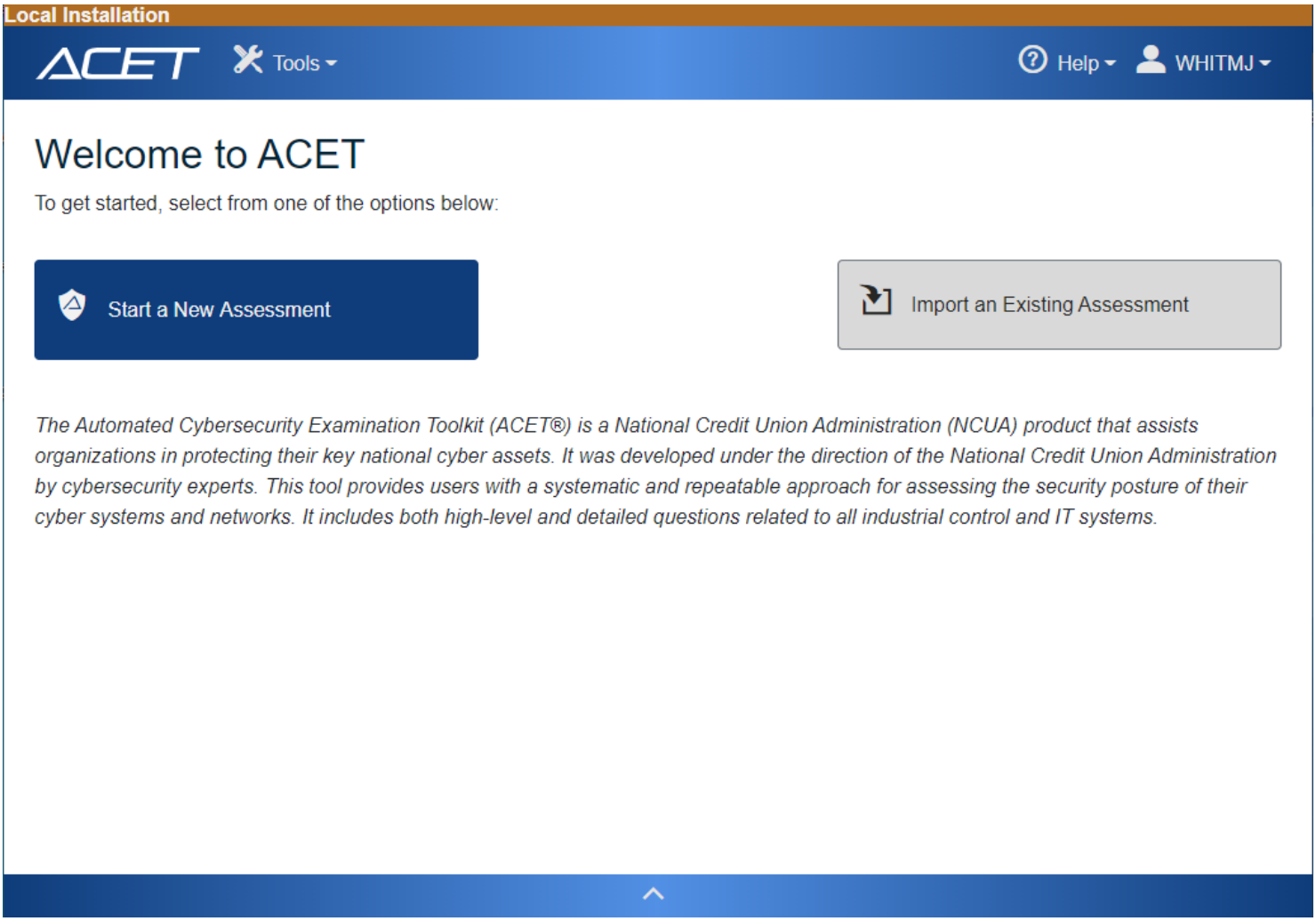


Figure: Local Install Landing Page

Using the Stand-alone

There are a few things users should know in regards to the stand-alone install of ACET.

Using the ACET System Tray Application

The ACET system tray app will be available in the user's task bar. To use it click the ACET icon .

The user will have the option to Open ACET Web, Start ACET Web, Stop ACET Web, Configure/Status, or Exit.

Selecting "Open ACET Web" will open a web instance of ACET.

Selecting "Start ACET Web" will run the application. If the application is already running the Start ACET Web option will not be available, and the user should see in the Configure/Status that the Status is "Running".

Selecting "Stop ACET Web" will end the application.

Selecting "Configure/Status" will open the ACET Web- Local Configuration and Status box. The user can utilize this to change their port, check the status of the application, or check the output log.

Figure: Local Configuration and Status box

Selecting the "Exit" option will close the ACET system tray application menu.

Differences Between the Local and Web Versions of ACET

When using the stand-alone a gold ribbon that says "Local Installation" is displayed. See the figure below.

In the User Profile menu there is only the option to go to "My Assessments". User's can't alter their profile information while in stand-alone mode. They will see their Windows NT user name displayed as their name.

Emails are not available while in stand-alone. All email functionality is in the web-based version of ACET.

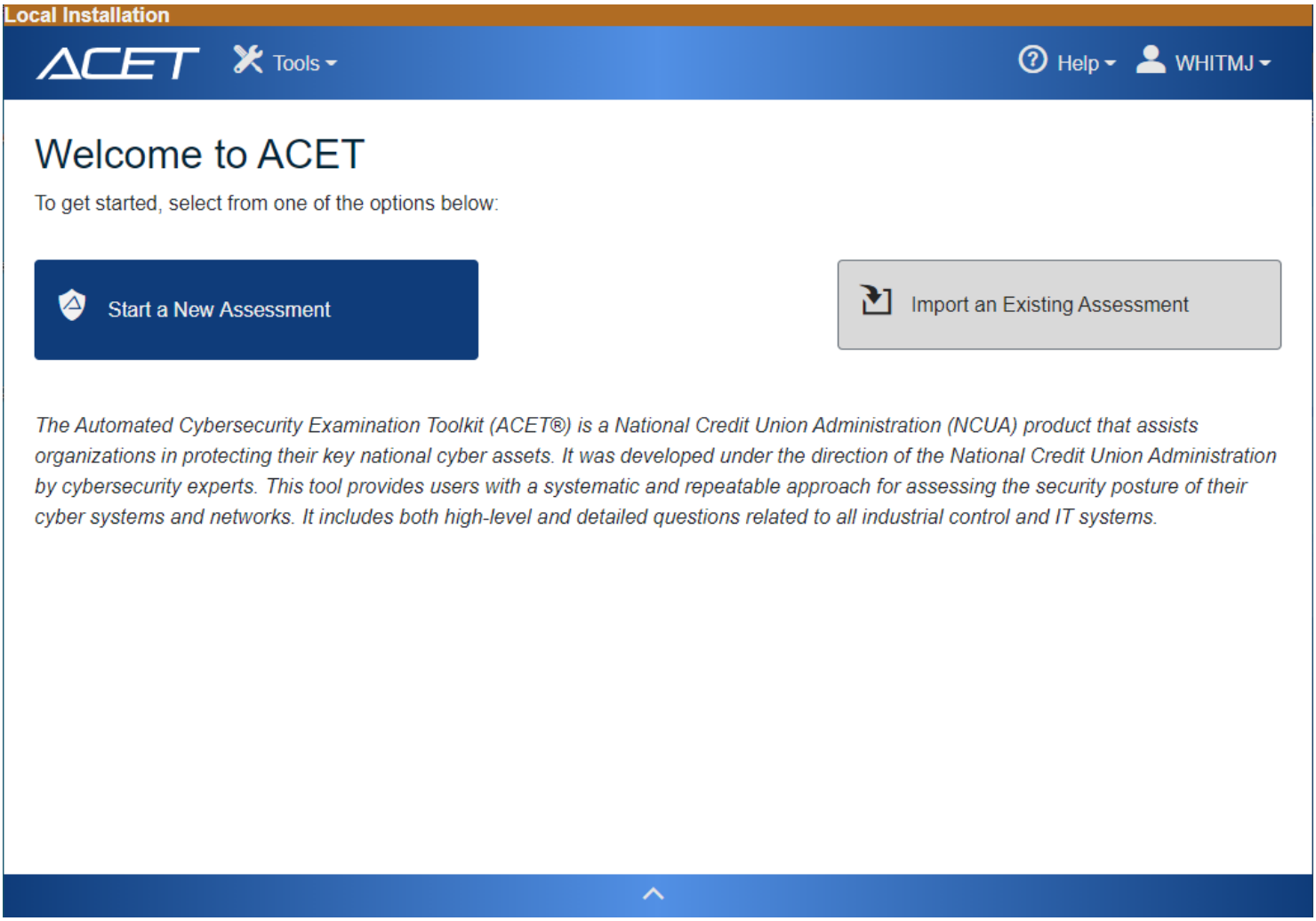


Figure: Stand-alone Landing page

Evaluation Preparation

Two preliminary tasks are required before using the tool to perform an assessment: (1) forming the subject matter team and (2) collecting the network/architecture documentation and related information.

Subject Matter Team Selection

The first step is to select a cross-functional assessment team consisting of subject matter experts selected from various operational areas in the organization. Organizations may add additional team members as needed to address specific topics. Anyone in the organization who has had training or experience with the ACET tool should be included on the team.

The primary user should spend some time using the ACET tool with test only or dummy data prior to commencement of the team activity. Familiarity with the ACET tool will improve speed and ease of use.

Representatives from the following areas are suggested for an effective assessment. The representatives should have significant expertise in their areas of responsibility.

For either an ICS or IT assessment:

- IT Network/Topology (knowledge of IT infrastructure).
- IT Security/Control System Security (knowledge of policies, procedures, and technical implementation).
- Risk Management (knowledge of the organization's risk management processes and procedures).
- Business (knowledge of budgetary issues and insurance postures).
- Management (a senior executive sponsor/decision maker).

If performing an ICS assessment:

- Industrial Control Systems (knowledge of industrial control system architecture and operations)
- System Configuration (knowledge of systems management).
- System Operations (knowledge of system operation).

Gather Supporting Documentation and Information

Previous ACET users have found that the following types of documents and information are useful to have during completion of the assessment. Collecting this reference information before beginning the assessment is advisable:

- Organizational chart that outlines responsibilities;
- Annual operating and capital budgets;
- Insurance policy description;
- Previously performed risk and vulnerability assessments;
- Capacity, operation, management, and maintenance manuals;
- Risk management documentation;
- Hazardous waste operations and emergency response Standards;
- Emergency Operations Plan/Emergency Response Plan;
- Asset inventory and criticality rating from Computerized Maintenance Management System (CMMS);
- Inventory list of process control/SCADA software and hardware, including interfaces;
- Network topology diagram and supporting documentation;
- Documentation/knowledge from previous incidents or near misses;
- General asset inventory, criticality asset determination, business impact analyses, contingency plans, etc.; and
- Information security policies, plans, and procedures.

When the assessment team is prepared and supporting documents are gathered, the organization is prepared to start ACET and begin the actual evaluation.

Start ACET

Go to http://localhost:46050/index.html or for other installation options the instructions provided in the help section titled Installation Procedure should be followed.
The actual URL maybe provided by your companies ACET administrator.

The ACET Home Screen will be displayed as seen in the figure below.

Figure: ACET Home Screen

Register a User Account

To get started in ACET you must have a registered account.

First, select the "Register New User Account" link. The Register Account dialogue will open.

Figure: Using the Home page to register an account

1 Login Email and Password fields

To login enter the user's email and password here.

2 Forgot Password link

This link opens a dialogue for user's to get a new temporary password and reset their old forgotten password.

3 Register Account link

This link will open a dialogue for the user to create a new account.

4 Login button

Click the login button after entering user information to login.

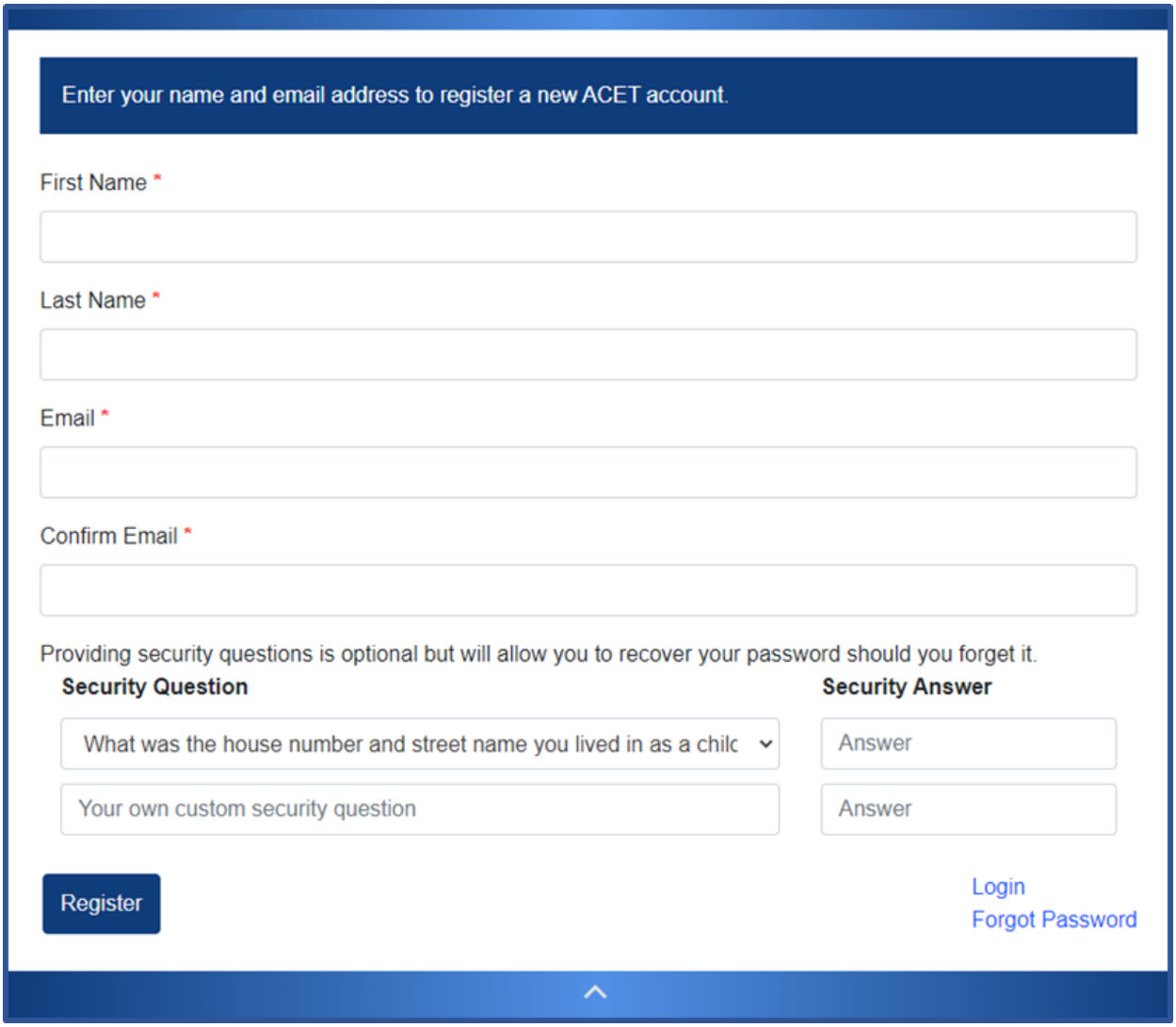


Figure: Registration dialogue

The user should enter their first and last name and email.

Users have the option to add security questions next. They are not required but will be another step in ensuring their identity when resetting a password. Users can select a question from the dropdown or create a custom question.

Select the "Register" button. The user will be sent an email with a temporary password and instructions to login. Users can navigate to ACET through the email or select the "Login" link on the dialogue above.

Note: Users can't register an email that has already been registered.

Import/Export a ACET Assessment

There are two different ways to import a ACET assessment.

Pick an option below to learn more.

Importing a .acet File

With the web-based version of ACET a user can import a .acet file. To begin click the Import button to begin the process.

Figure: Import Button

The user's File Explorer will open, and at this point they can select a .acet file. A new assessment that is a duplicate of the uploaded assessment will show in the user's landing page.

NOTE: The web-based version of ACET only supports .acet file upload. Legacy file (.cset) upload is not supported.

Exporting an ACET Assessment

To export an assessment simply select the Export button next to the assessment to be exported on the Landing page.

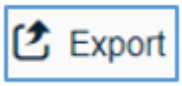


Figure: Export button

After clicking the Export button the assessment will be downloaded as a .acet file and will be in the user's Downloads folder (unless otherwise specified in browser settings).

Title Bar

The Title Bar allows the user to access high-level functions of the ACET application and is shown in the figure below.

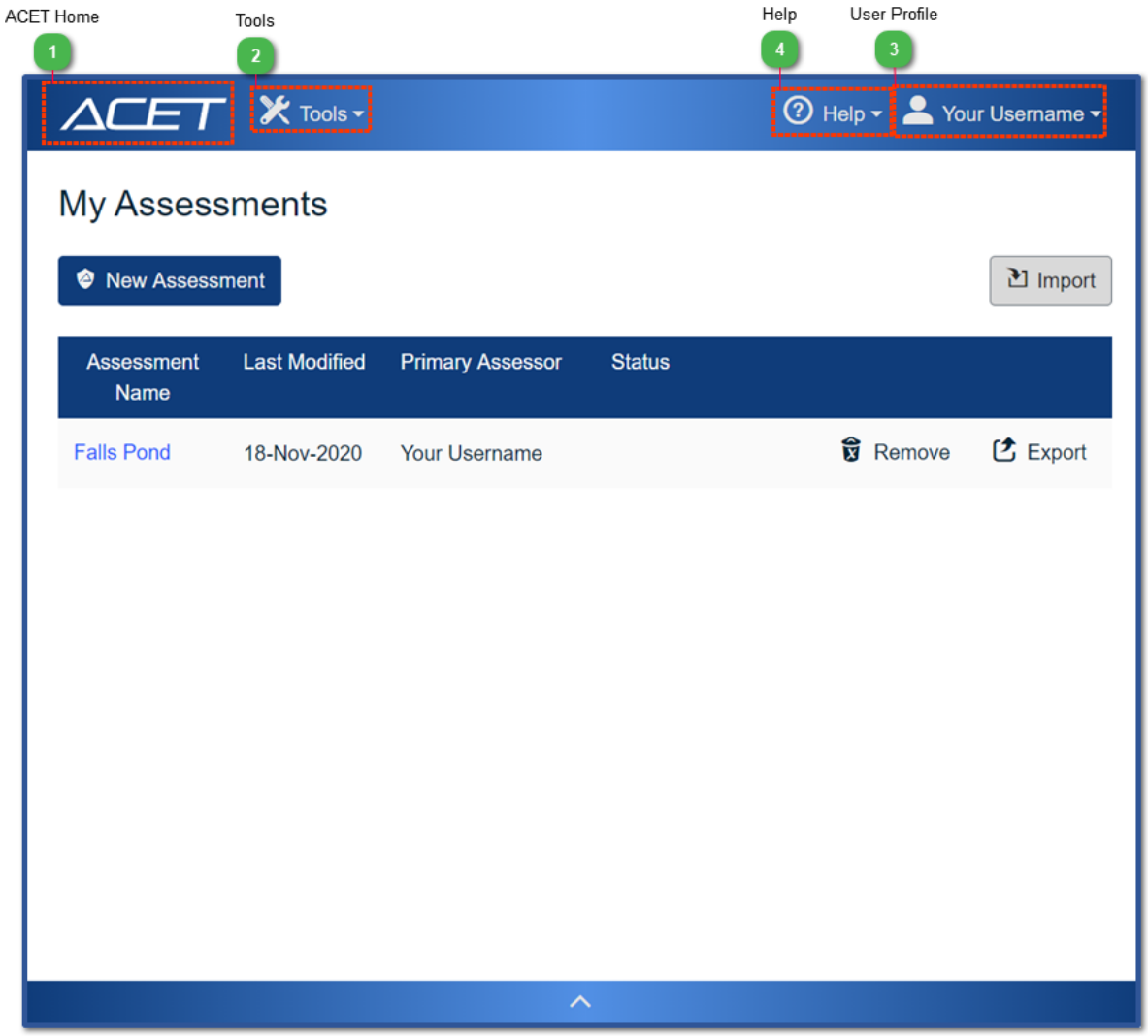


Figure: Title Bar

1 ACET Home

The ACET HOME button opens the user's landing page.

For more information about the landing page, see the Landing Page help section.

2 Tools

The Tools button opens the Tools menu.

For more information about the Tools menu, see the Tools Menu help section.

3 User Profile

(This will display your user name)

The User Profile button opens the User Profile menu.

For more information about the User Profile menu, see the User Profile help section.

4 Help

The Help button opens the Help menu.

For more information about the Help menu, see the Help Menu section.

Tools Menu

The Tools Menu provides the user with options outside of the assessment process. The user can access the Enable Protected Features, Parameter Editor, Export Assessment to Excel, and Advanced features. The Tools Menu is described in the figure below.

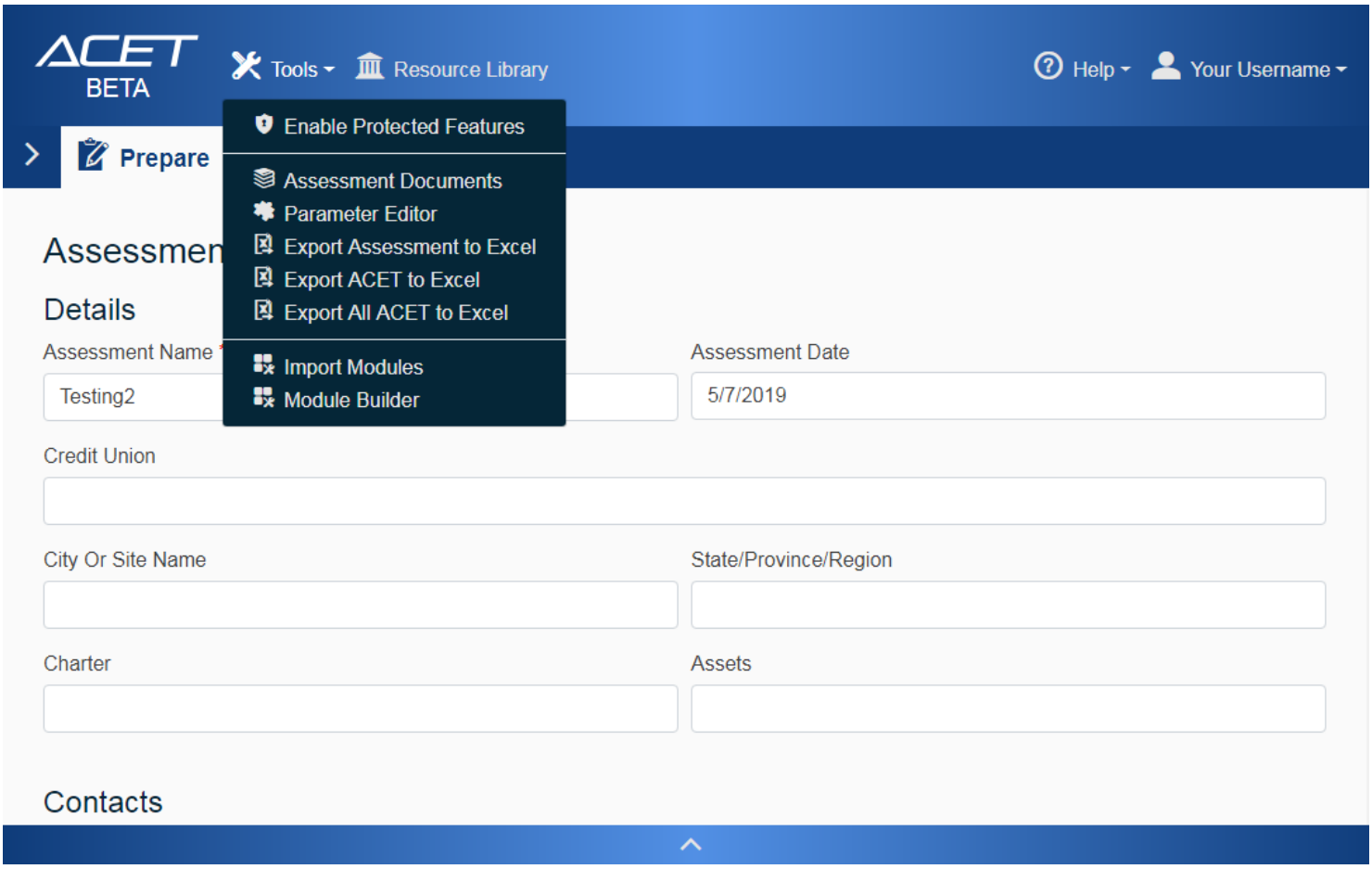
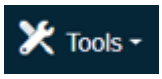


Figure: Tools Menu

Click the Tools menu button 

to open the Tools menu.

Enable Protected Features: Clicking the Enable Protected Features menu item displays the Protected Features window that allows the user to view specific questionnaires or standards developed by specific industries that are not available to the general public.

See Protected Features for more information.

Parameter Editor: Clicking the Parameter Editor menu item displays the Parameter Editor window where users can maintain parameters related to their selected Standard in requirements mode, if they are supported.

See Parameter Editor more information.

Export to Excel: Clicking the Export to Excel menu item downloads an excel spreadsheet with the answers to the assessment Questions or Requirements.

See Export to Excel for more information.

Export to ACET to Excel: Clicking the Export ACET to Excel downloads a single ACET assessment.

See Export ACET to Excel for more information.

Export All ACET to Excel: Clicking the Export All ACET to Excel link downloads all ACET assessments on the user's landing page to a single excel sheet.

See Export All ACET to Excel for more information.

Import Module: The Import Modules menu item holds the Import Module feature used for custom standard import.

See Import Module for more information.

Module Builder: Clicking the Module Builder menu item opens the Module Builder feature that users can build new question and requirements sets.

See Module Builder for more information.

NOTE: The Assessment Documents, Parameter Editor, and Export to Excel features are not available unless within an assessment. If on the landing page the Tools menu will look like the figure below.

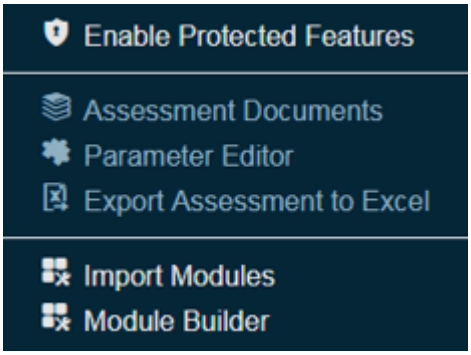


Figure: Tools menu outside of an assessment

Parameter Editor

Many Cybersecurity Standards in ACET contain parameter information in the requirement text. Parameters are indicated by [ ] symbols in the requirement text. For example, the SP800-53 R4 App J Standard contains the following parameter: [Assignment: organization-defined frequency, at least annually].

The Default Parameter Editor allows the user to replace the default parameter text with other text the user defines. So in the previous example, the user might replace the [Assignment: organization-defined frequency, at least annually] parameter with the word Annually. The Default Parameter Editor will then replace all occurrences of the parameter with the user's text.

Users can also change the parameters within the Requirement text itself with inline parameter editing. Simply click in to the parameter edit and save.

The Default Parameter Editor window is described in the figure below.

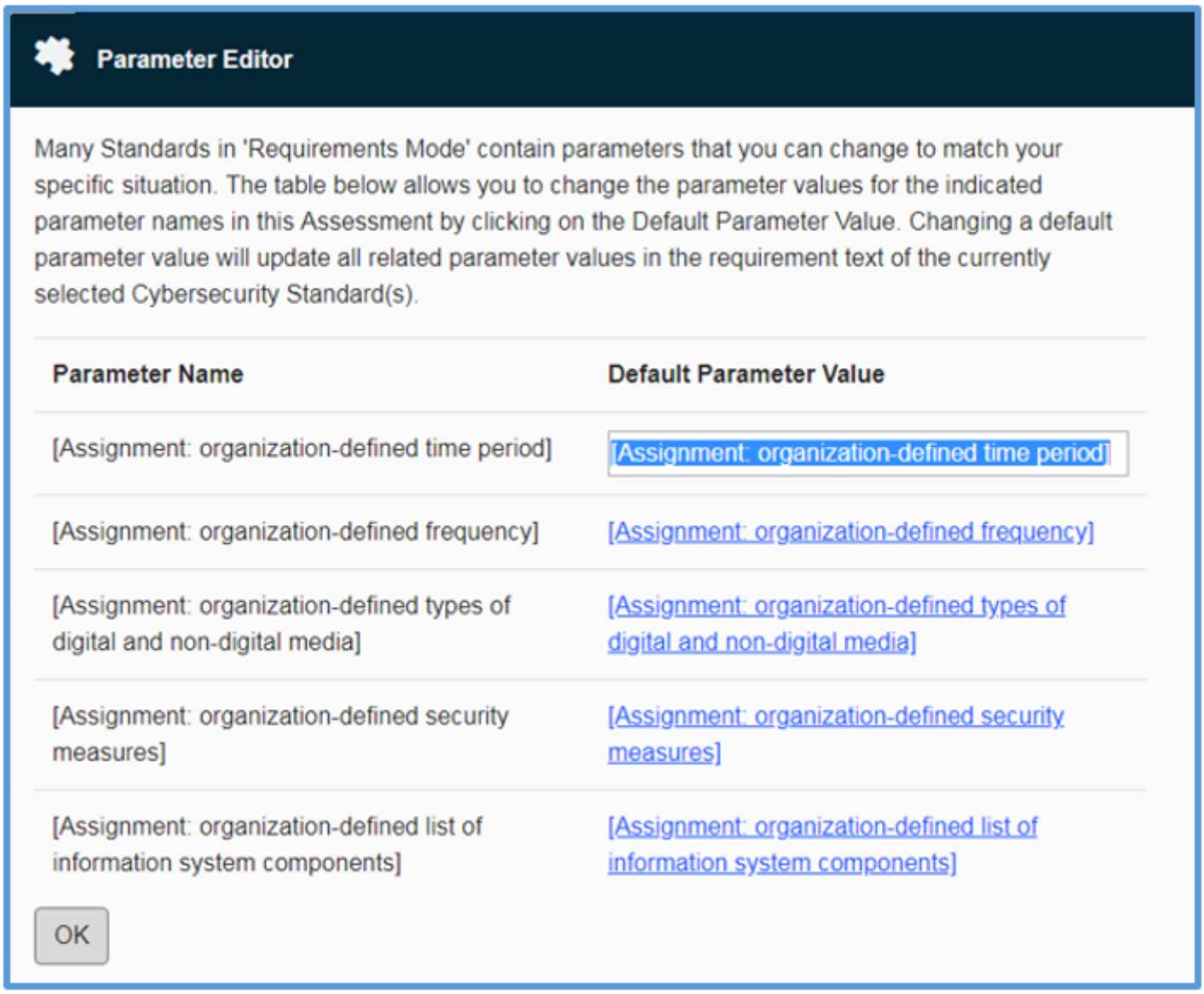


Figure: Default Parameter Editor Window

Parameter List: The Parameter List displays a list of Parameter Names and associated Default Parameter Values.

The Parameter Name column shows the name of the parameter and cannot be changed.

The Default Parameter Value column displays the current parameter values associated with the parameter names for the selected Standards as seen in the Requirement text on the Assessment screen. The parameter values are initially the same as the Parameter Name but can be changed by the user. To change a parameter value, double-click the cell containing the desired Default Parameter Value and enter new parameter text. Perform the same with any other parameters. Once finished, click the "Ok" button.

All parameter values in the requirement text will then be updated with the entered text for the given parameter names throughout the assessment.

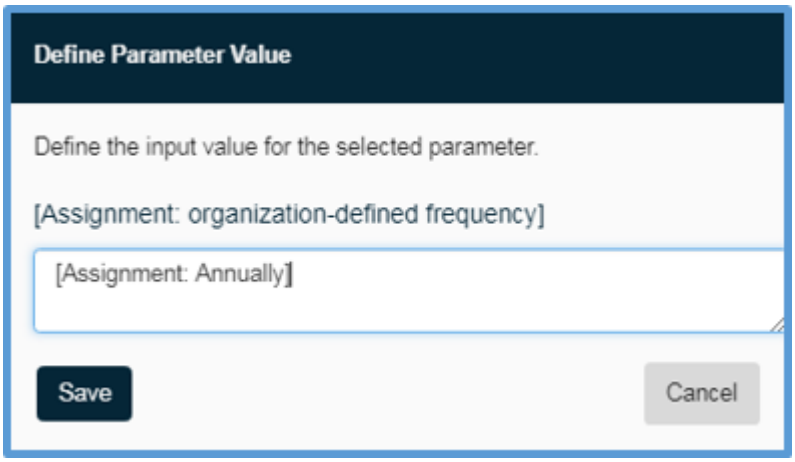


Figure: Inline Parameter Editing

Protected Features

The Protected Features window allows the user to add a feature unlock code to release specific standards or questionnaires that are not available to the general public. The Protected Features window is described in the figure below.

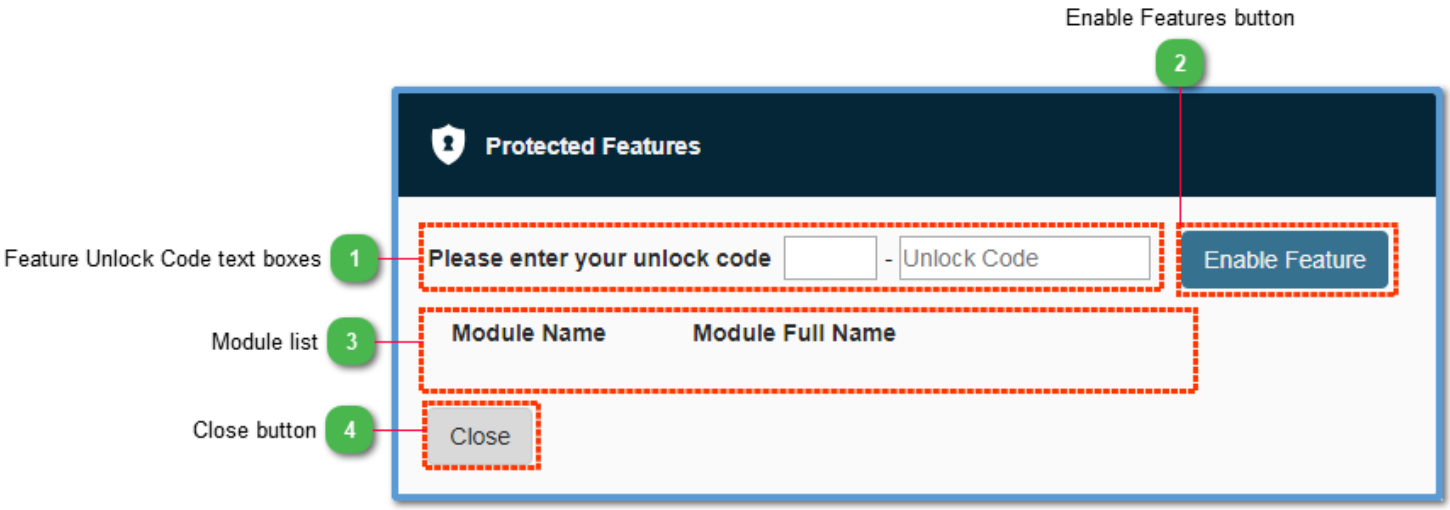
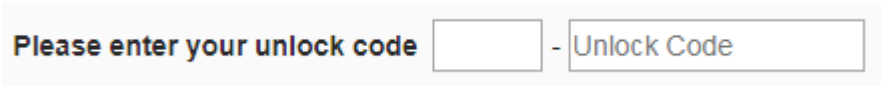


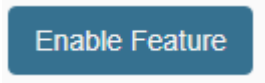
Figure: Protected Features Window

1 Feature Unlock Code text boxes



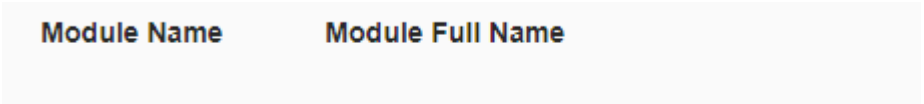
The Feature Unlock Code input text boxes allow the user to enter the feature unlock code. Once a proper code has been entered, the Module List will display all available standards or questionnaires that can be added to the ACET Standards Selection screen.

2 Enable Features button



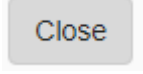
Select the Enable Feature button after entering the Unlock Code.

3 Module list



The Module List displays a list of available standards or questionnaire modules that are unlocked and available in the Cybersecurity Standards Selection page.

4 Close button

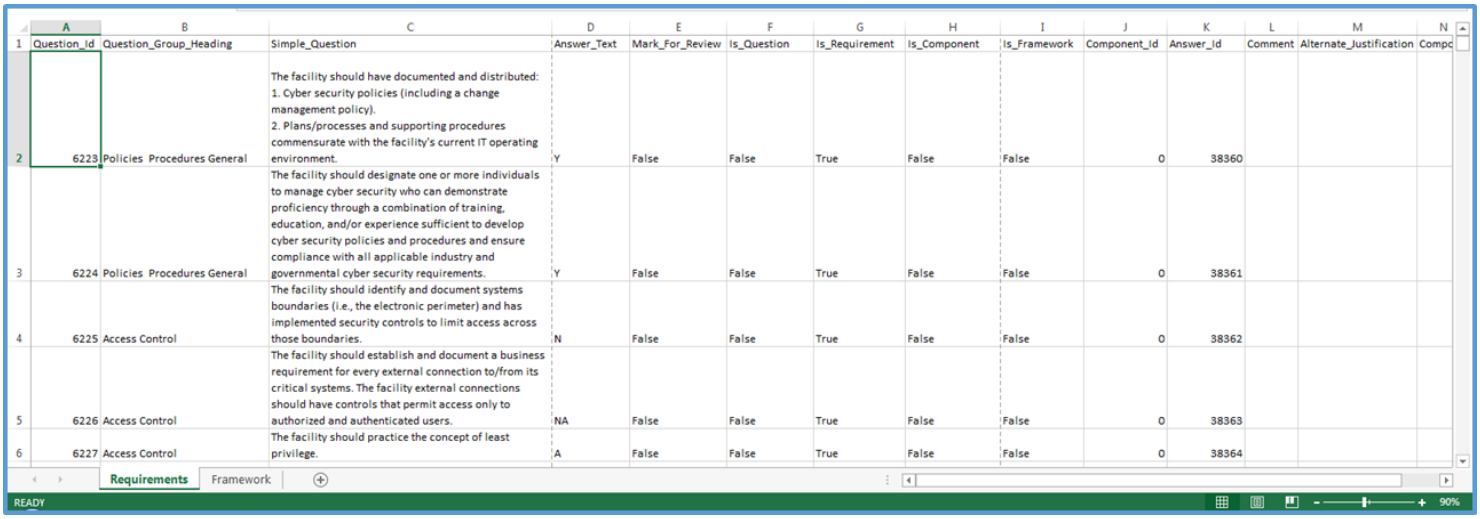


The Close button closes the Protected Features dialogue and commits changes.

Export to Excel

Selecting the "Export to Excel" link will download an excel copy of your assessment results.

NOTE: The excel report shows either Questions or Requirements. Whichever mode has more answers will show in the report.

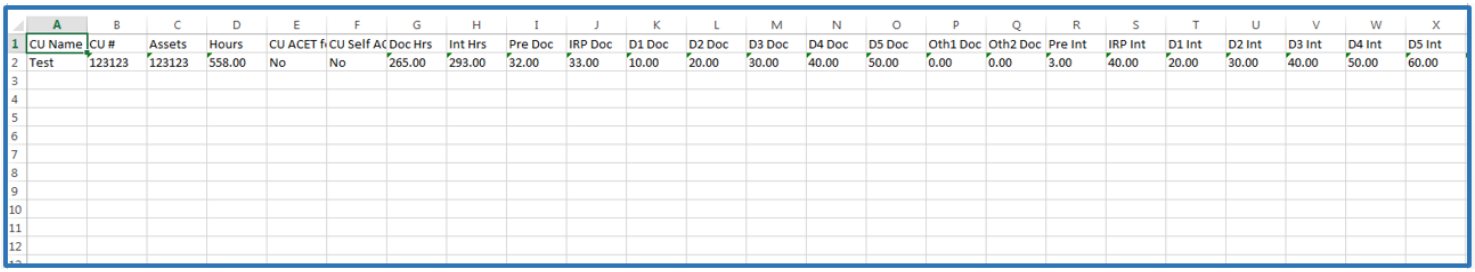


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Question_Id	Question_Group_Heading	Simple_Question	Answer_Text	Mark_For_Review	Is_Question	Is_Requirement	Is_Component	Is_Framework	Component_Id	Answer_Id	Comment	Alternate_Justification	Compc
2	6223	Policies Procedures General	The facility should have documented and distributed: 1. Cyber security policies (including a change management policy). 2. Plans/processes and supporting procedures commensurate with the facility's current IT operating environment.	Y	False	False	True	False	False	0	38360			
3	6224	Policies Procedures General	The facility should designate one or more individuals to manage cyber security who can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop cyber security policies and procedures and ensure compliance with all applicable industry and governmental cyber security requirements.	Y	False	False	True	False	False	0	38361			
4	6225	Access Control	The facility should identify and document systems boundaries (i.e., the electronic perimeter) and has implemented security controls to limit access across those boundaries.	N	False	False	True	False	False	0	38362			
5	6226	Access Control	The facility should establish and document a business requirement for every external connection to/from its critical systems. The facility external connections should have controls that permit access only to authorized and authenticated users.	NA	False	False	True	False	False	0	38363			
6	6227	Access Control	The facility should practice the concept of least privilege.	A	False	False	True	False	False	0	38364			

Figure: Export to Excel Output

Export ACET to Excel

Selecting the "Export ACET to Excel" link will download an excel copy of your assessment results. This sheet mimics the Data Sheet found in the ACET Workbook.

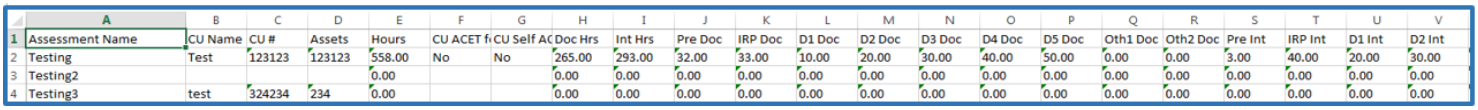


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	CU Name	CU #	Assets	Hours	CU ACET fi	CU Self AC	Doc Hrs	Int Hrs	Pre Doc	IRP Doc	D1 Doc	D2 Doc	D3 Doc	D4 Doc	D5 Doc	Oth1 Doc	Oth2 Doc	Pre Int	IRP Int	D1 Int	D2 Int	D3 Int	D4 Int	D5 Int
2	Test	123123	123123	558.00	No	No	265.00	293.00	32.00	33.00	10.00	20.00	30.00	40.00	50.00	0.00	0.00	3.00	40.00	20.00	30.00	40.00	50.00	60.00
3																								
4																								
5																								
6																								
7																								
8																								
9																								
10																								
11																								
12																								

Figure: Export ACET to Excel

Export All ACET to Excel

Each row represents an assessment so that all of your assessment data exists in a single sheet. Selecting "Export All ACET to Excel" downloads all ACET assessments from the My Assessments screen.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	Assessment Name	CU Name	CU #	Assets	Hours	CU ACET fi	CU Self AC	Doc Hrs	Int Hrs	Pre Doc	IRP Doc	D1 Doc	D2 Doc	D3 Doc	D4 Doc	D5 Doc	Oth1 Doc	Oth2 Doc	Pre Int	IRP Int	D1 Int	D2 Int
2	Testing	Test	123123	123123	558.00	No	No	265.00	293.00	32.00	33.00	10.00	20.00	30.00	40.00	50.00	0.00	0.00	3.00	40.00	20.00	30.00
3	Testing2				0.00			0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	Testing3	test	324234	234	0.00			0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figure: Export all ACET

Import Module

NOTE: The Import New Module is designed for Developer use. The user needs experience with either JSON or XML.

There are a few different options to import a new Questions or Requirements set in ACET. The user can use an edit an existing standard, create their own JSON or XML module in ACET, or use a schema in an outside code editor and paste in ACET.

The parts of the Import New Module can be seen in the figure below.

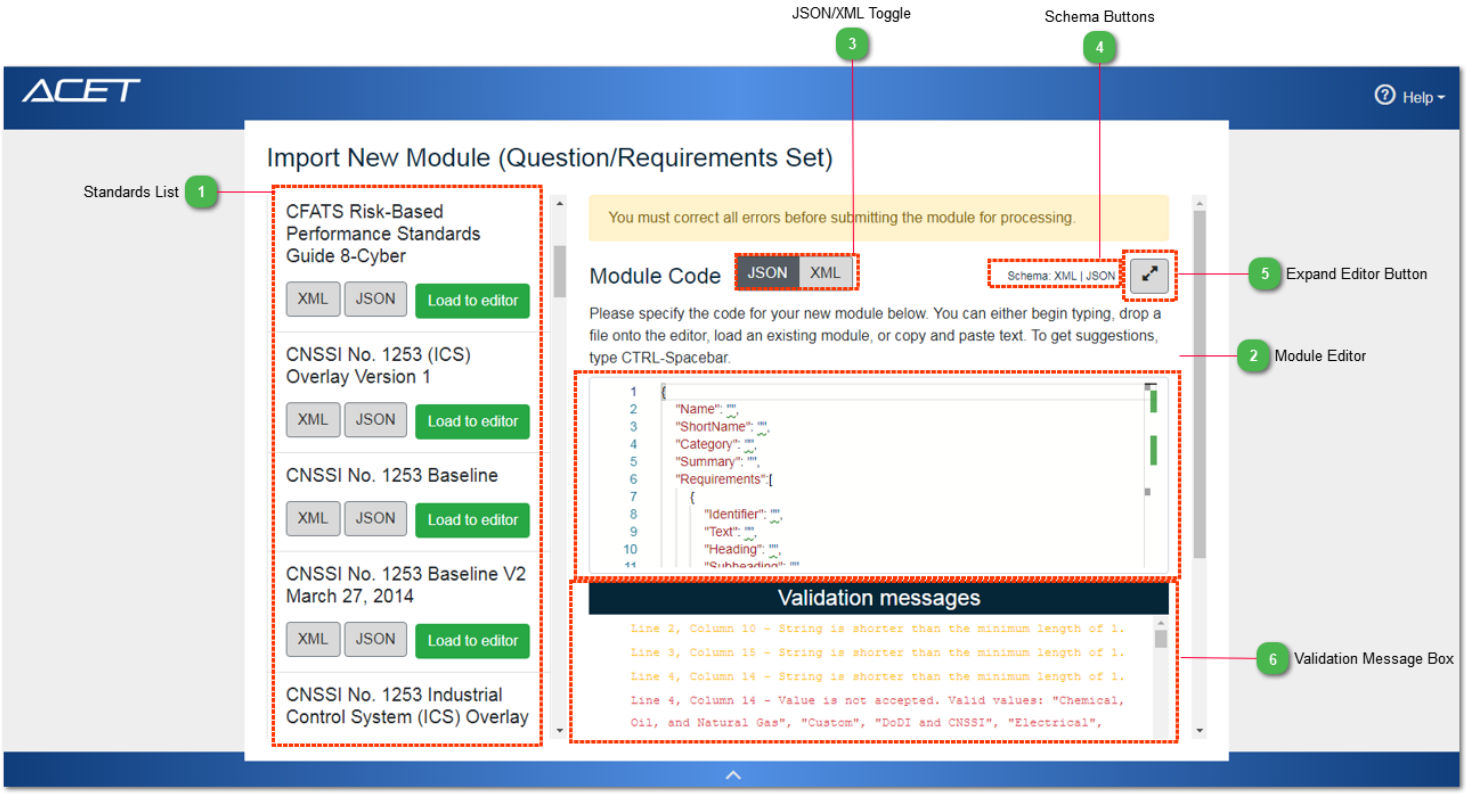
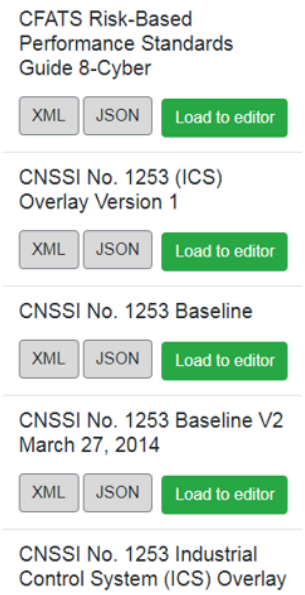


Figure: Import New Module screen

1 Standards List



The Standards List allows the user to export any of the standard code in either XML or JSON. It also allows the user to click "Load to editor" to load any standard code to the Module Editor where it can be edited. When a new standard is imported it will show in the Standard List, as well as, the Cybersecurity Standards page.

2 Module Editor

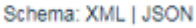
The Module Editor is where the user can edit or create a new standard for import. Edit within the tool or drag and drop a file to the editor.

Tip: Use CTRL+Spacebar to see list options while coding. Use ALT+Shift+F to format code when loaded from the Standards List.
Note: New Standards can contain both Questions and Requirements. If only using Requirements they will be duplicated for the Questions set.
Short Names must be unique when editing a previously used standard.

3 JSON/XML Toggle

Use the JSON/XML Toggle to pick what language to use for the new standard being imported. It is recommended to use JSON, because ACET has more comprehensive validation and list options within the editor.

4 Schema Buttons

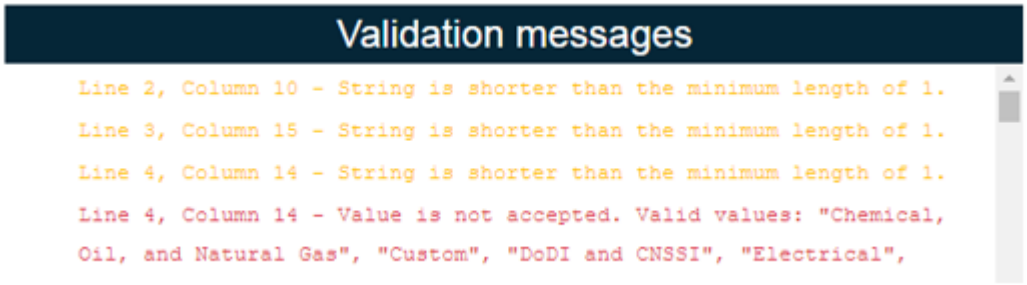


Use the Schema button to download a code schema to edit in an outside editor. Drag and drop the file when complete to see validation messages and submit.

5 Expand Editor Button

Click the Expand button to expand the Module Editor to the full-screen.

6 Validation Message Box



The Validation Message box shows errors in the code, as well as, processing errors.

Add Reference Documents: Users can add supporting documents and references with the newly created standard. Drop reference files into the reference file drop area, enter a title, and a short name. Use the red trash icon or remove all to delete supporting documents.

Tip: If using the Destinations field in the editor to direct a user to a certain place in the supporting document, then the destinations must be set up in the support document itself. See Choose Your Destination for more information.

Module Builder

The Module Builder allows the user to create a custom Standard or Question Set.

Module List

The Module List displays all custom modules. A custom module is one that is not included in the ACET application.

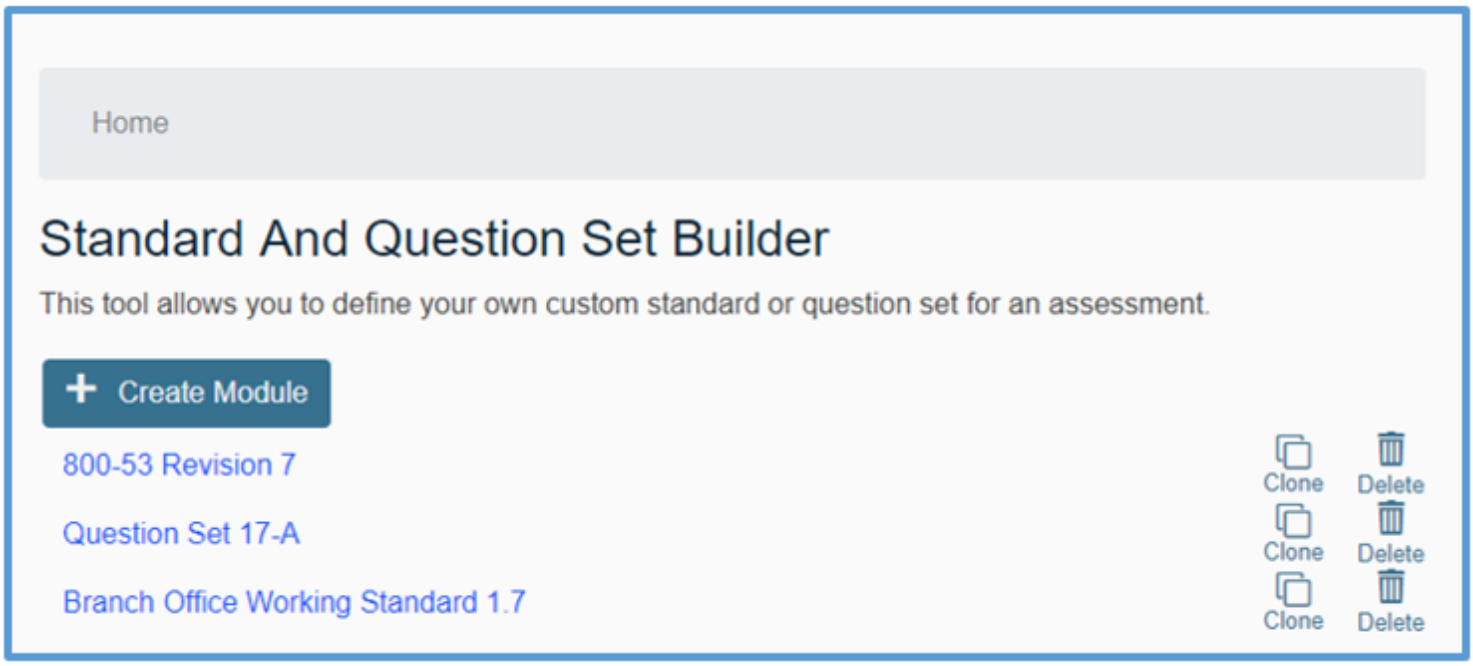


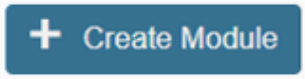
Figure: Module list

Clone Button 

A module can be cloned by clicking this button. A deep copy of the module is created including requirements and questions. The source module's title is copied to the new clone, appending "(copy)". The user is transferred to the Module Detail page for the new clone.

Delete Button 

A custom module may be deleted, provided that no other modules have requirements based on it. This is enforced to maintain data integrity.

Create Module Button 

Clicking the Create Module button will start the construction of a new module. The user is transferred to the Module Detail page.

Create a New Module

After clicking the "Create Module" button the Module Detail screen will open.

Module Detail

The Module Detail screen contains basic information about the module, such as name and description.

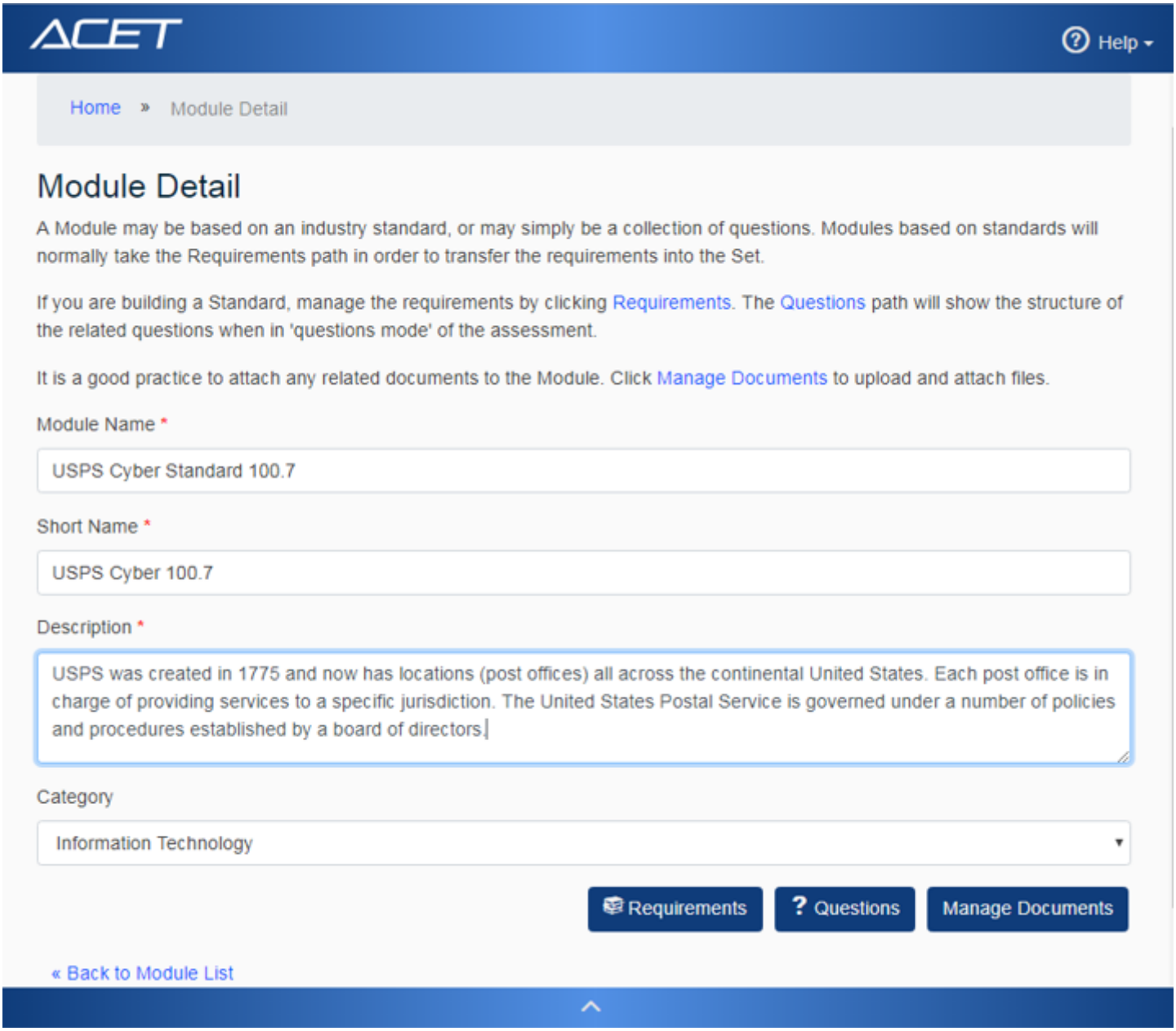
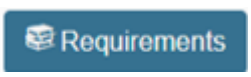


Figure: Module Detail screen

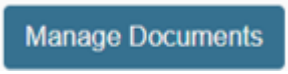
Requirements Button 

Clicking the Requirements button will show the Requirement Listing screen.

Questions Button 

Clicking the Questions button will show the Questions List screen.

Manage Documents



Clicking the Manage Documents button will show the Standard Documents screen.

Add Requirements

Clicking the Requirements button opens the Requirement Listing screen where the user can add a new requirement to their set.

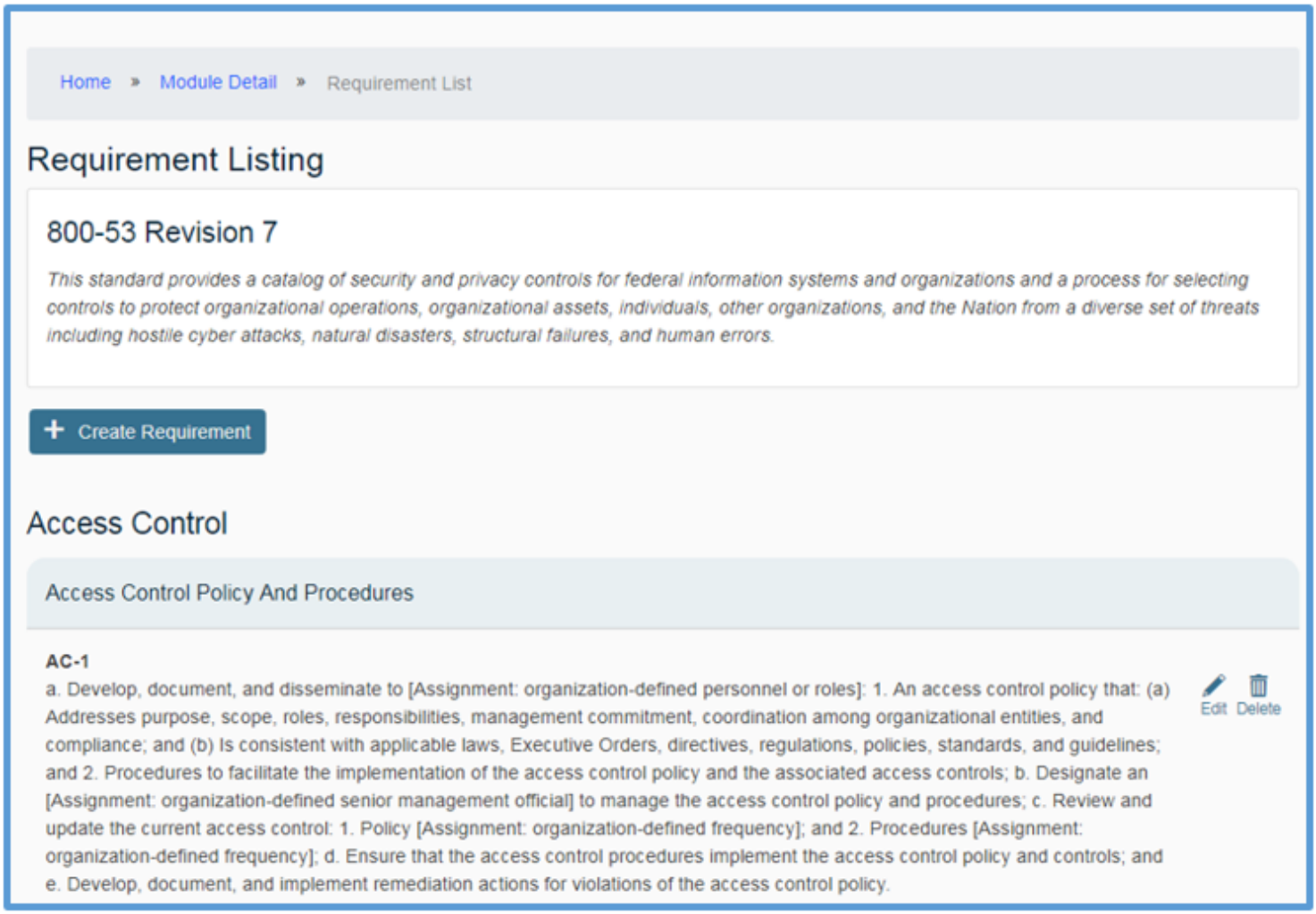


Figure: Requirement Listing screen

Select the Create Requirement button to open the Add requirement dialogue.

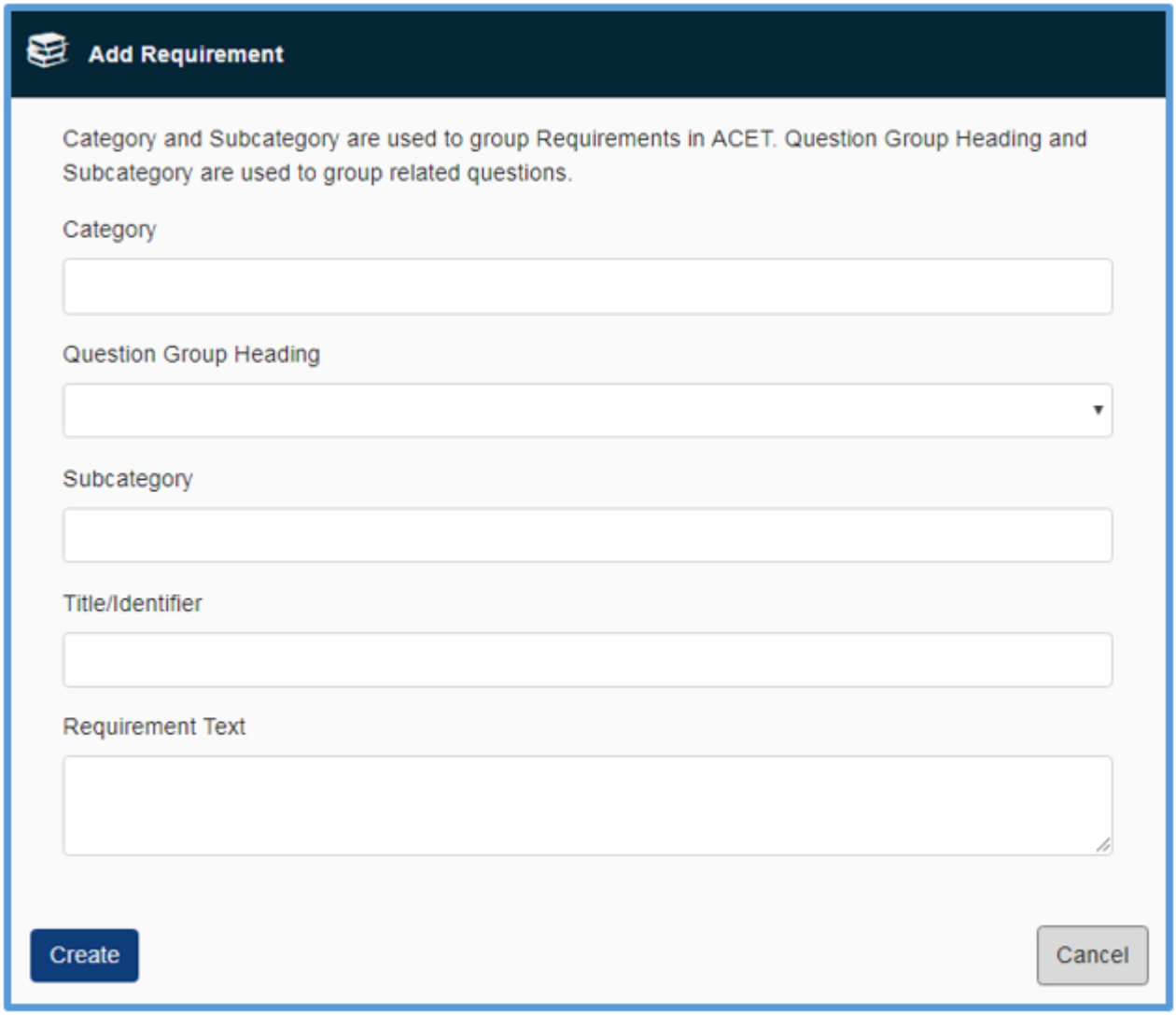


Figure: Add a Requirement dialogue

Category Dropdown list: Select or enter the control group category. Typing in this field will filter the dropdown values to matching values.

For more information about question categories, see the Assessment Categories help section.

Question Group Heading Dropdown list: This is a value under which questions are grouped when displayed in ACET questions mode.

For more information about question group headings, see the Assessment Categories help section.

Subategory Dropdown list: Select or enter the control subcategory.

For more information about question subcategories, see the Assessment Categories help section.

Title/Identifier field: Enter the title or identifier of the Requirement. For example, Requirement 1 (Req.1).

Requirement Text field: Enter the full text of the Requirement. Line breaks are preserved for readability and are presented when answering in ACET Requirements mode.

Create button: Click the Create button to save the new requirement and jump to the Requirement Detail screen.

Requirement Detail

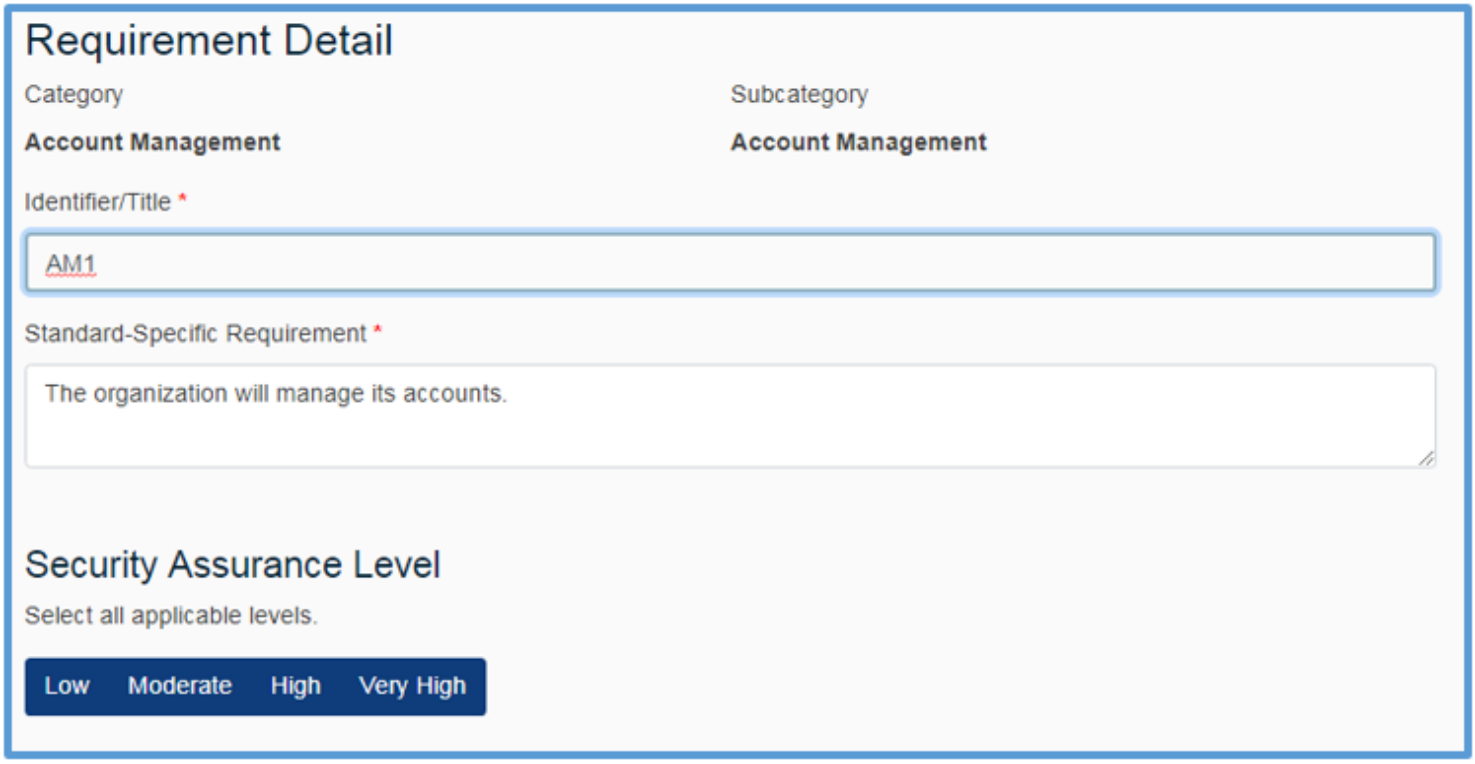


Figure: Requirement Details and SAL level

The values for Identifier/Title and the Requirement text are editable on this screen as well.

Security Assurance Level: Select all Security Assurance Levels that are applicable to the Requirement.

For more information about Security Assurance Levels, see the Security Assurance Level (SAL) help section.

Next, add any supplemental information for the requirement.

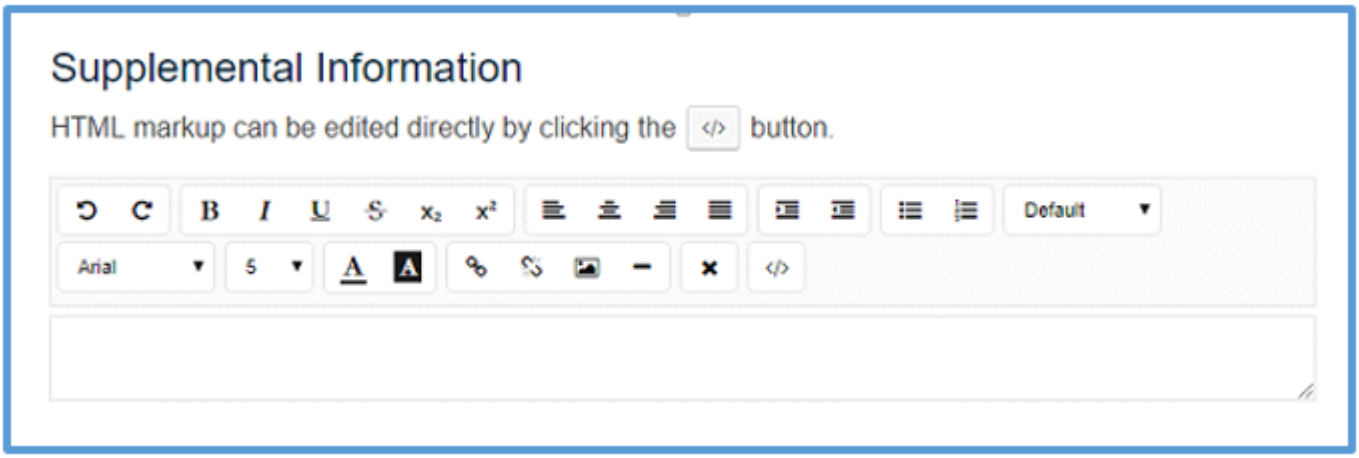


Figure: Supplemental text box

Supplemental Information text box: Enter any supplemental information for the Requirement in this box. The text can be formatted using the controls and can be edited directly as HTML by clicking the </> button.

References

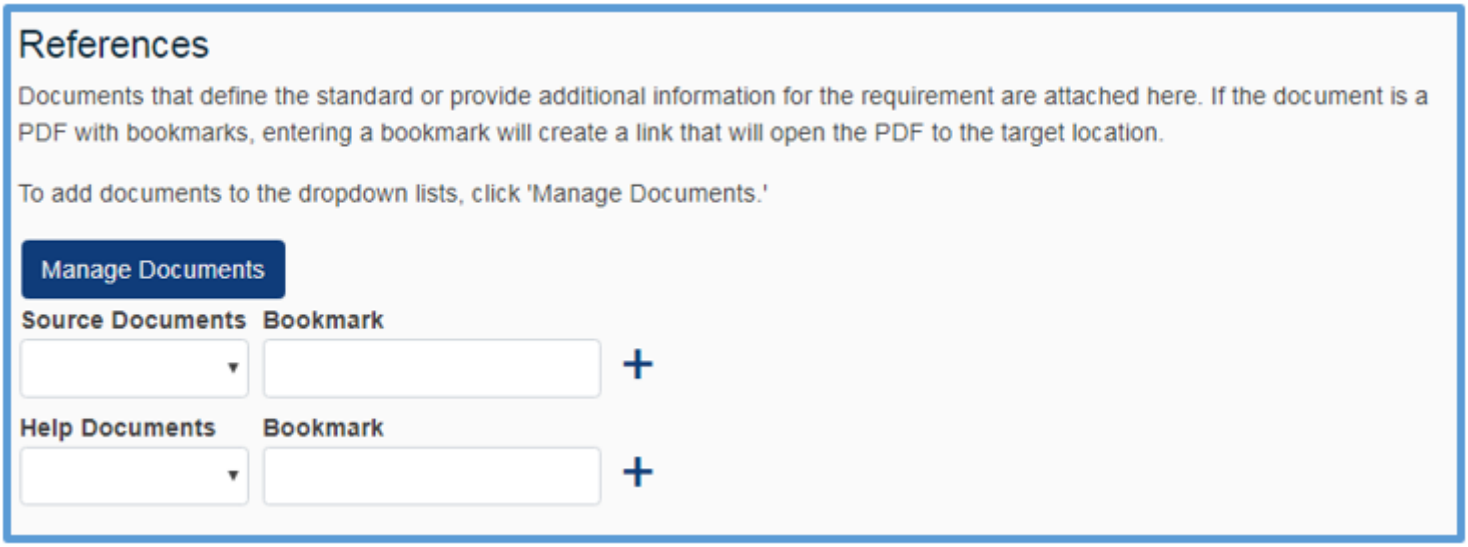


Figure: Add and manage documents

Manage Documents button: Before a reference document can be connected to a Requirement it must first be associated with the Module. Click this button to jump to the Standard Documents List, where that connection can be made.

Source Documents dropdown list: A Source Document is the primary location that supplies the Requirement for the Standard. Documents that have been associated with this Module will be listed here.

Bookmark: Optional. ACET will render hyperlinks in the References section of the Requirements screen. For convenience, those links will open the Reference or Help document and jump directly to a pre-defined bookmark. If there is a bookmark in the document, it can be entered here. Enter the bookmark without a leading hash/pound symbol (#).

Click the '+' button to add the reference to the Requirement. Multiple references can be added to a Requirement.

Help Documents dropdown list: A Help Document is a secondary source of information that may be helpful to the assessor to help understand a Requirement. They are added the same way as Source Documents, and are listed separately on the Requirements screen in ACET.

At this point the user can add simple questions to the individual requirement, so that they can utilize both Questions and Requirements mode. (This is not required)

To learn more about Questions/Requirements mode, see the Mode Selection help section.

Add Questions

A user can begin adding questions to a requirement through the Requirement Details screen. The Related Questions section is found at the bottom of the page.

To learn more about the Requirements Details screen, see the Add Requirements help section.

Figure: Add Related Questions

Questions can be assigned to a Requirement in order to define a question-based answer capture. This screen allows new questions to be written and attached, or questions can be pulled from the extensive set of questions defined in ACET.

For more information about Questions, see the Mode Selection help section.

Write New Question

If a question is needed that is not already defined in ACET, it may be created as shown in the figure below.

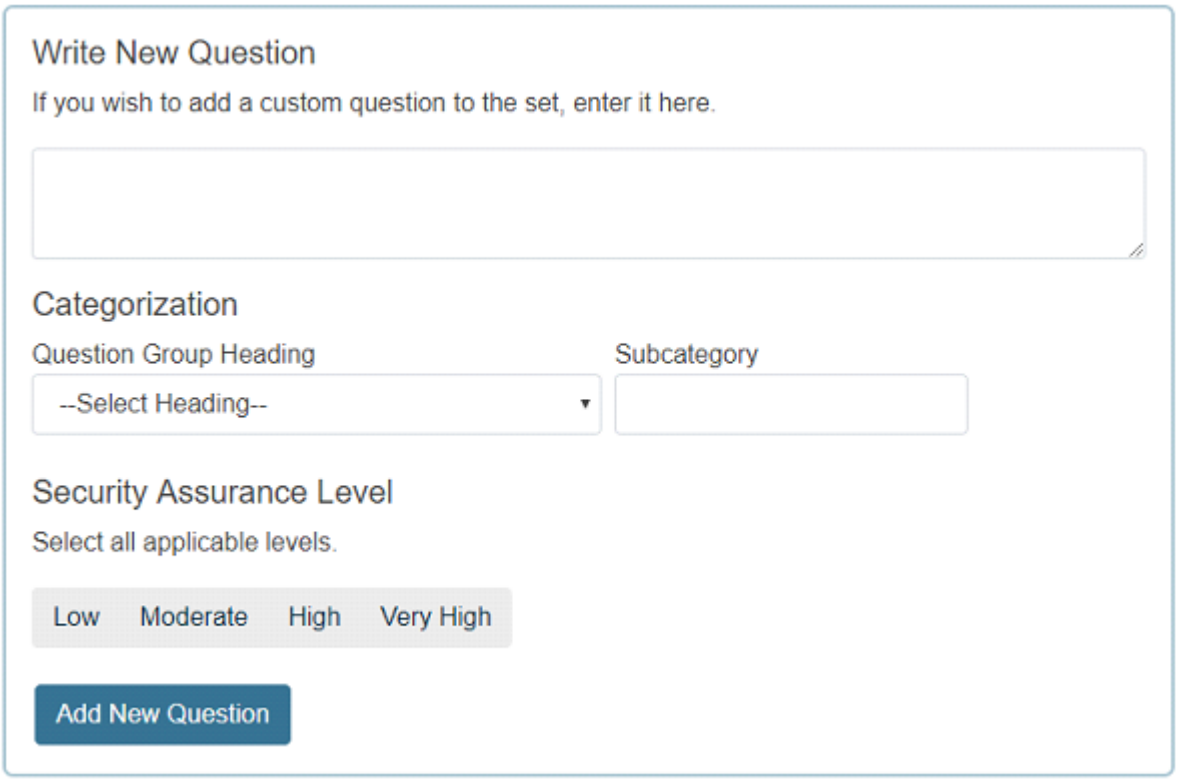


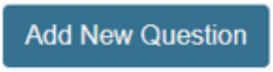
Figure: Write new question dialogue

Question text box: Write the text of the new question here.

Question Group Heading dropdown list: Select a Question Group Heading that categorizes the question.

Subcategory: Select or enter the control subcategory.

Security Assurance Level: Select all Security Assurance Levels that are applicable to the Question.

Add New Question button 

: Click to create the new question.

Search for Existing Questions

Enter keywords that would appear in the relevant question(s) and click the Search button. A list of candidates will be rendered. More words in the query will yield a smaller resulting set of questions.

Each question will display its Question Group Heading and Subcategory values, along with the Security Assurance Levels defined for the question in its original Module. You can leave them set as-is or change them as appropriate for the new Requirement.

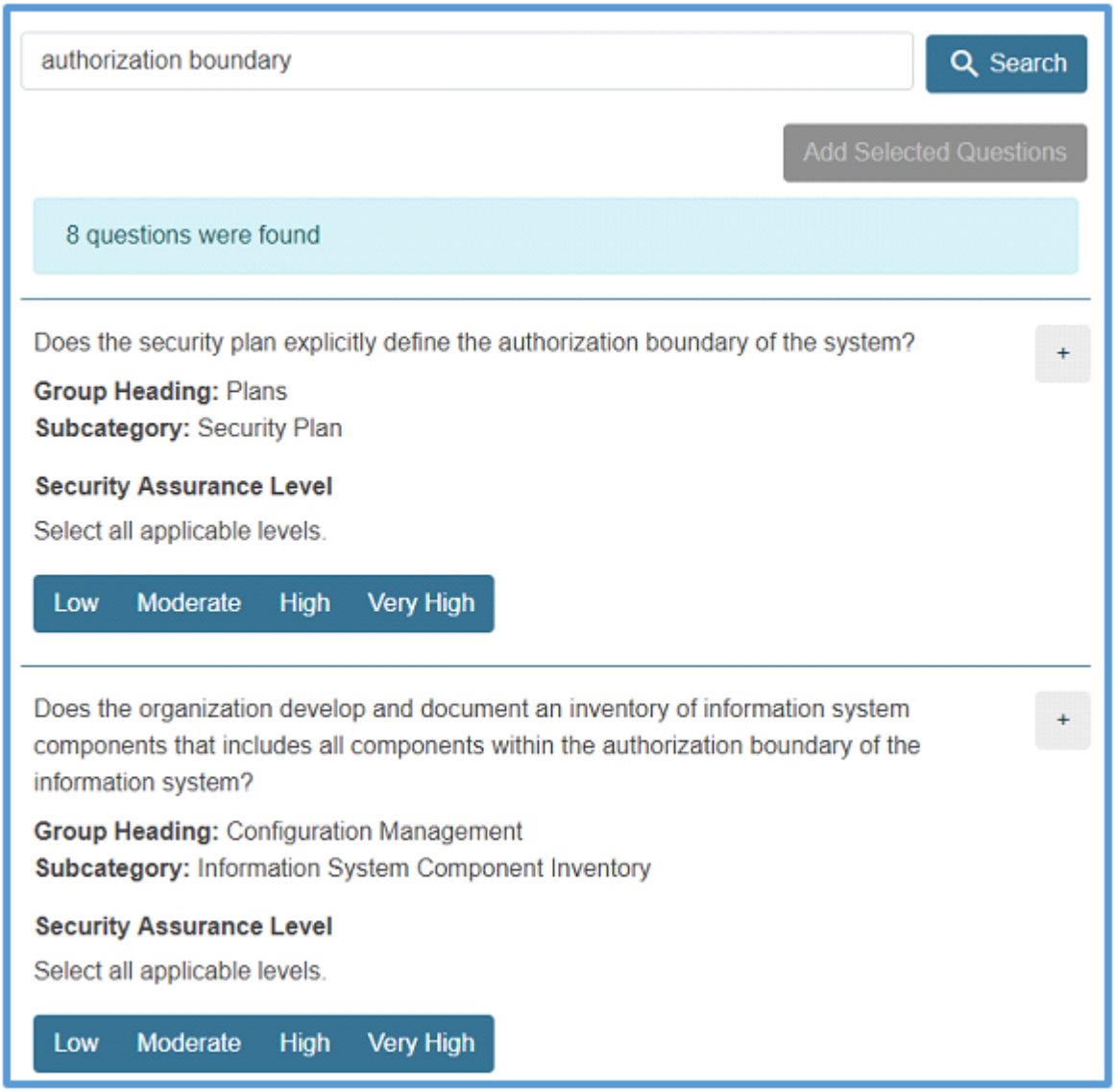


Figure: Searching for existing questions

Click the '+' button for each question that you wish to attach to the Requirement. Then click 'Add Selected Questions.'

Manage Documents

Standard Documents List

The Standard Documents screen lists all reference documents that are delivered with ACET or have been added to support custom modules.

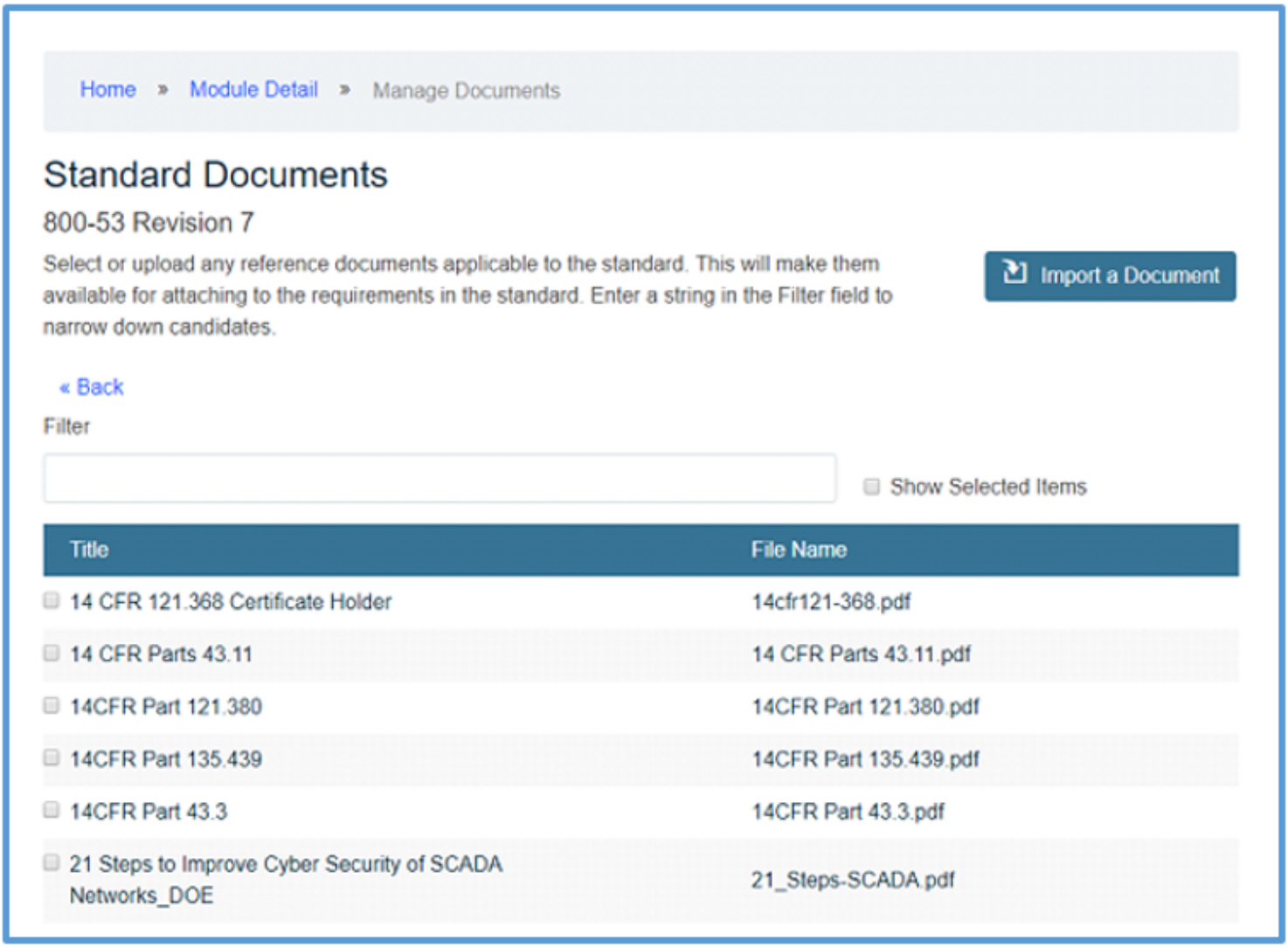


Figure: Standards document list

Import a Document Button

Opens a dialog to select a reference document for upload.

Filter

Typing in this field will trim the displayed list of documents to make it easier to locate the desired document.

List checkboxes

Any documents that should be available to associate with a Requirement, either as a Source Document or Help Document can be checked in this list.

NOTE: Checking a document in this list only makes the document available for inclusion when defining Requirements. To add a document to a Requirement, see the instructions for the Requirement Detail page.

Resource Library

The Resource Library is an excellent way to help the user better understand and resolve the concerns identified by the assessment and to improve the security of the user's systems. It contains a variety of Standards, reports, templates, white papers, plans, and other cybersecurity-related documents. The figure below shows the Resource Library window.

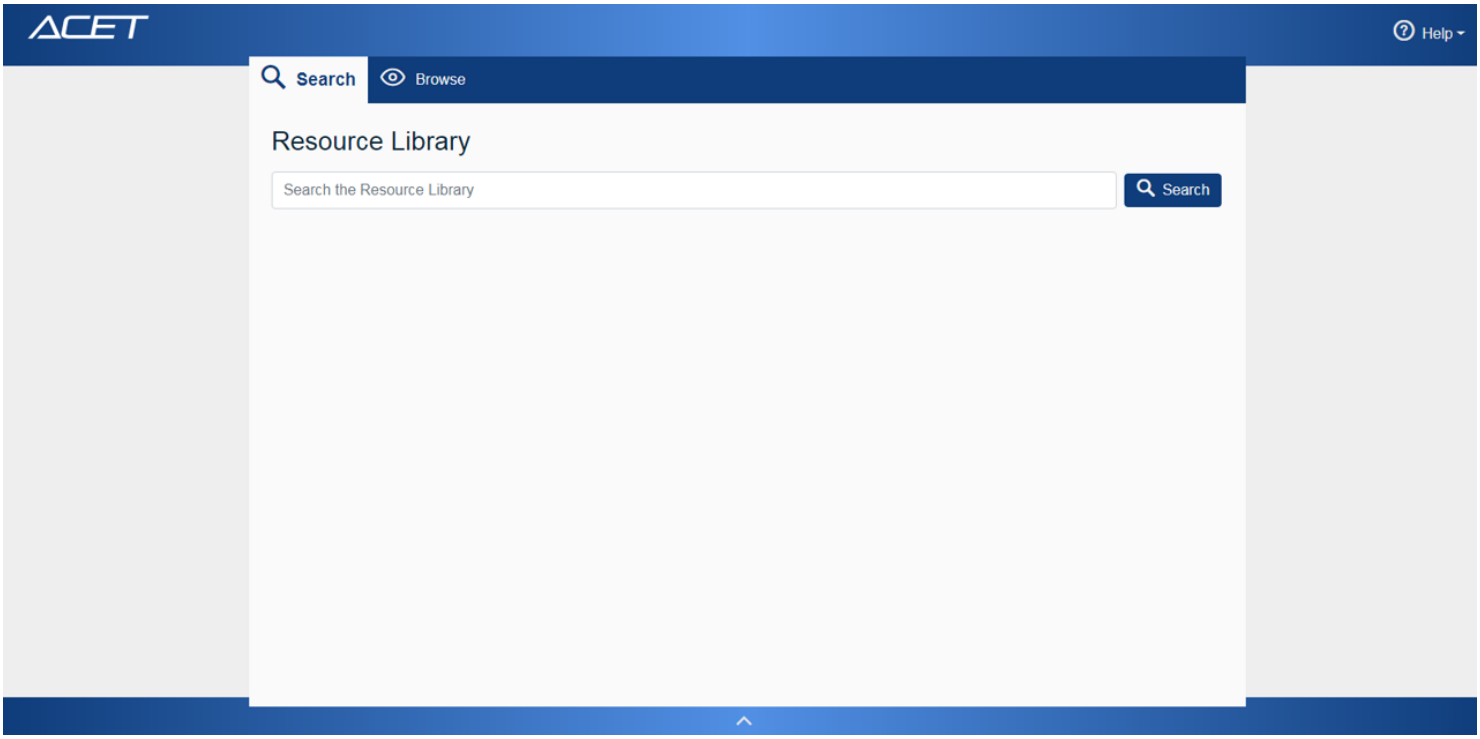


Figure: Resource Library Window

Search Screen

Two ways are available to find documents within the Resource Library. This section discusses the Search feature. The other way is by using the document tree structure discussed in the help section titled Browse Screen.

The Search screen option of the Resource Library provides a way to find a list of documents based on the text string typed into the search box. Clicking the Search tab opens a search box. Enter the desired text string and click on the magnifying glass icon or press the keyboard Enter key to begin the search.

The figure below shows an example where the user has typed in the string "testing." In this case, ACET searches through all the documents for occurrences of the word "testing" and then ranks and presents them in an ordered list in the Search Results.

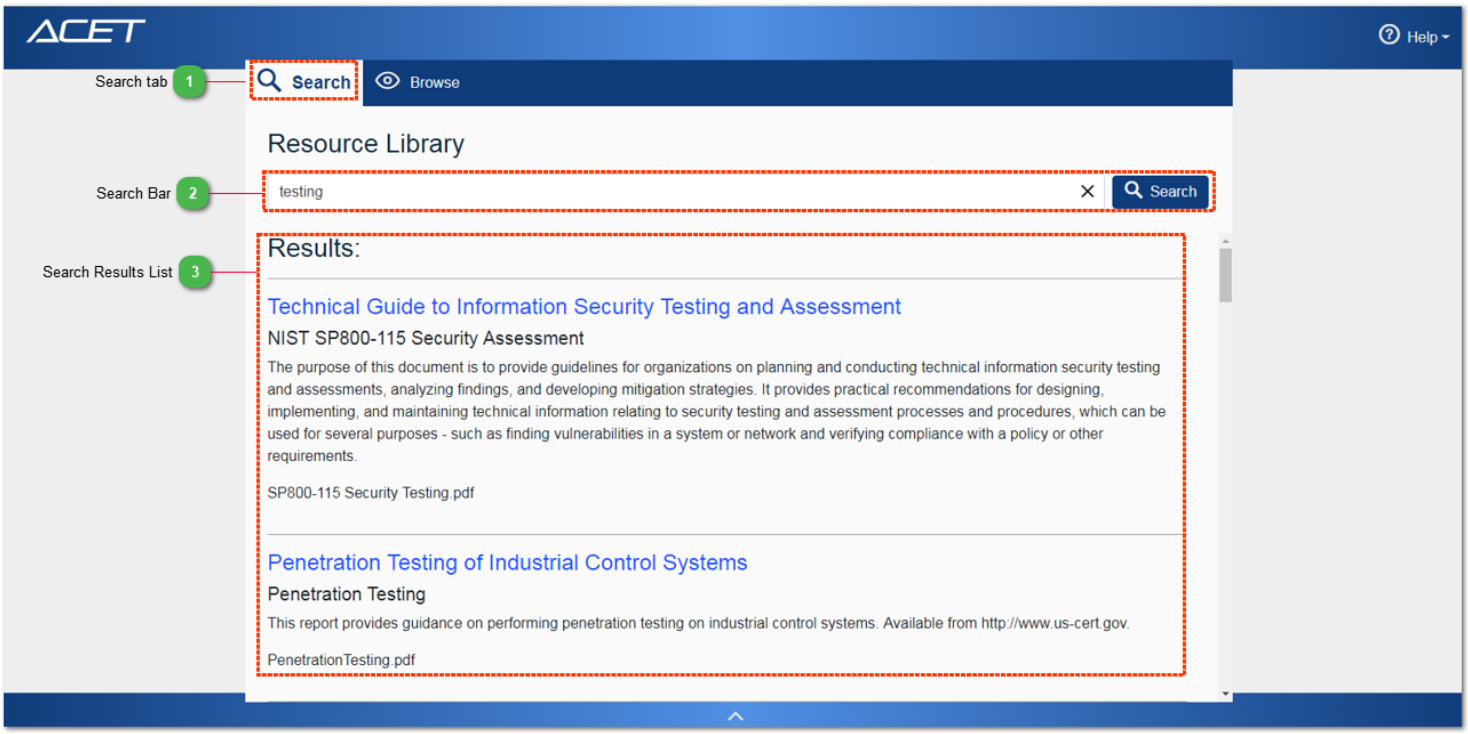
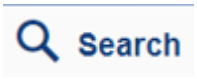


Figure: Resource Library Search Screen

1 Search tab

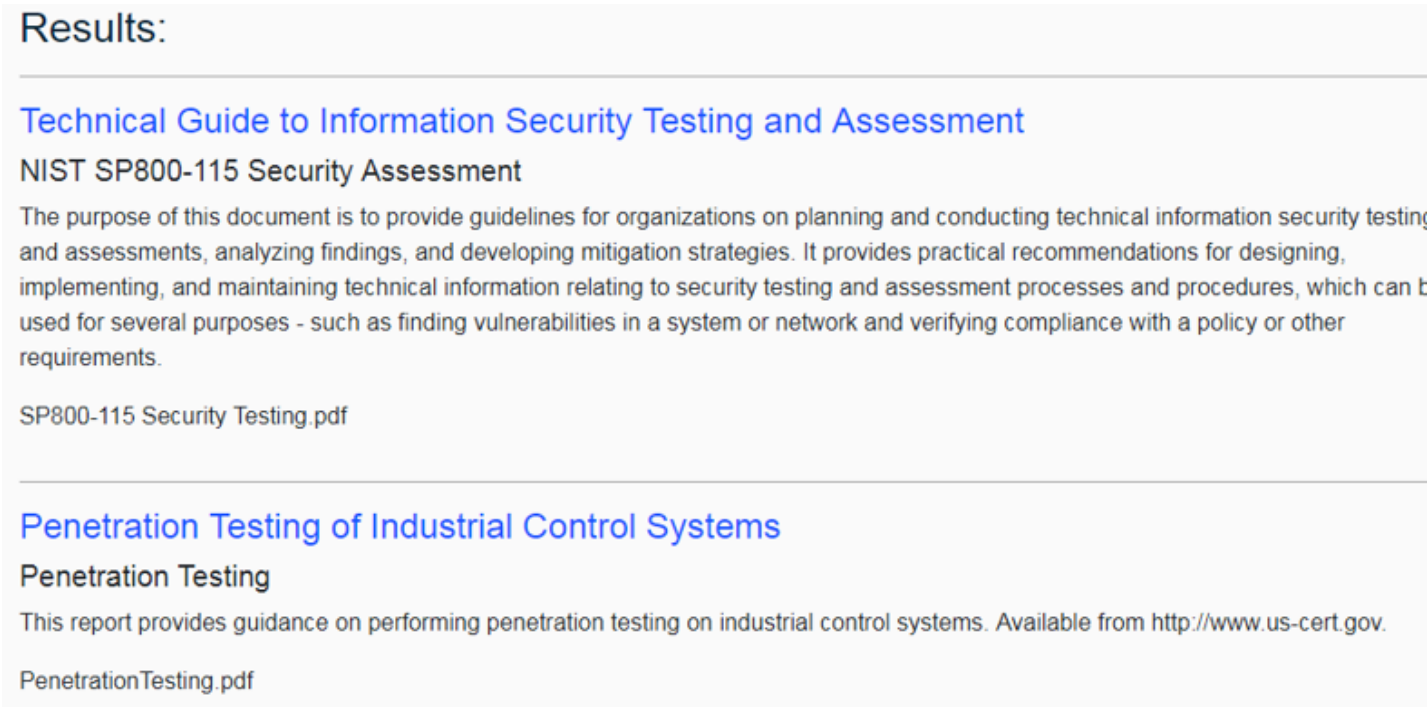


Clicking the Search tab will display the search functions of the Resource Library. The Resource Library always opens to the Search tab.

2 Search Bar

The Search bar allows the user to enter keywords related to the desired documents. The user enters one or m keywords
and clicks the Search button or presses the "Enter" key on the keyboard to perform the search. Results of the displayed in the Search Results list.

3 Search Results List



The Search Results list displays the documents found by the Search. Once there are documents displayed, the user can click a document to see the contents in a new tab.

Wildcards

There are two different types of wildcard characters that can be used in the search. The first is the asterisk character that can be used to substitute for one or more characters. For example, if entering the text "fire*", the search would look for anything starting with those characters and the user would see a prioritized list starting with topics related to firewalls. Without the asterisk the search would look for *"fire"* and the first entry would be Fire Protection.

Exact characters could also be substituted with question marks. For example, entering the text "*NIST SP800-??*" will return the NIST Special Publication 800 series documents where the last two characters are substituted by the wildcard character.

When ACET is searching for the text string, it is evaluating both the title and the content of the document. While the search will evaluate any character string, it is recommended that the entry be as specific as possible to limit and refine the list. The search is not sophisticated enough to find similar or close spellings. A misspelled word like "*Ciber-Security*" will return no results.

Topic Searches

In most cases, the user will be searching for a specific subject; however, the search capability can also be used to search for types of documents. In the example above, the returned document is a DHS recommended practice. By entering "recommended practice" in the search text box, the user can create a list of all the recommended practices developed by DHS as well as other documents that may use that phrase.

Browse Screen

Two ways are available to find documents within the Resource Library. The first is by using the Search screen discussed in the help section titled Search Screen. The second is by using the document tree structure shown in the figure below.

In the document tree structure, all the topics in the library are organized in a hierarchical format and displayed as leaf nodes on one or more branches, with a branch representing a topic. Each main topic can be expanded to more detailed subtopics until only the list of documents remains. The branches may be one or several levels deep.

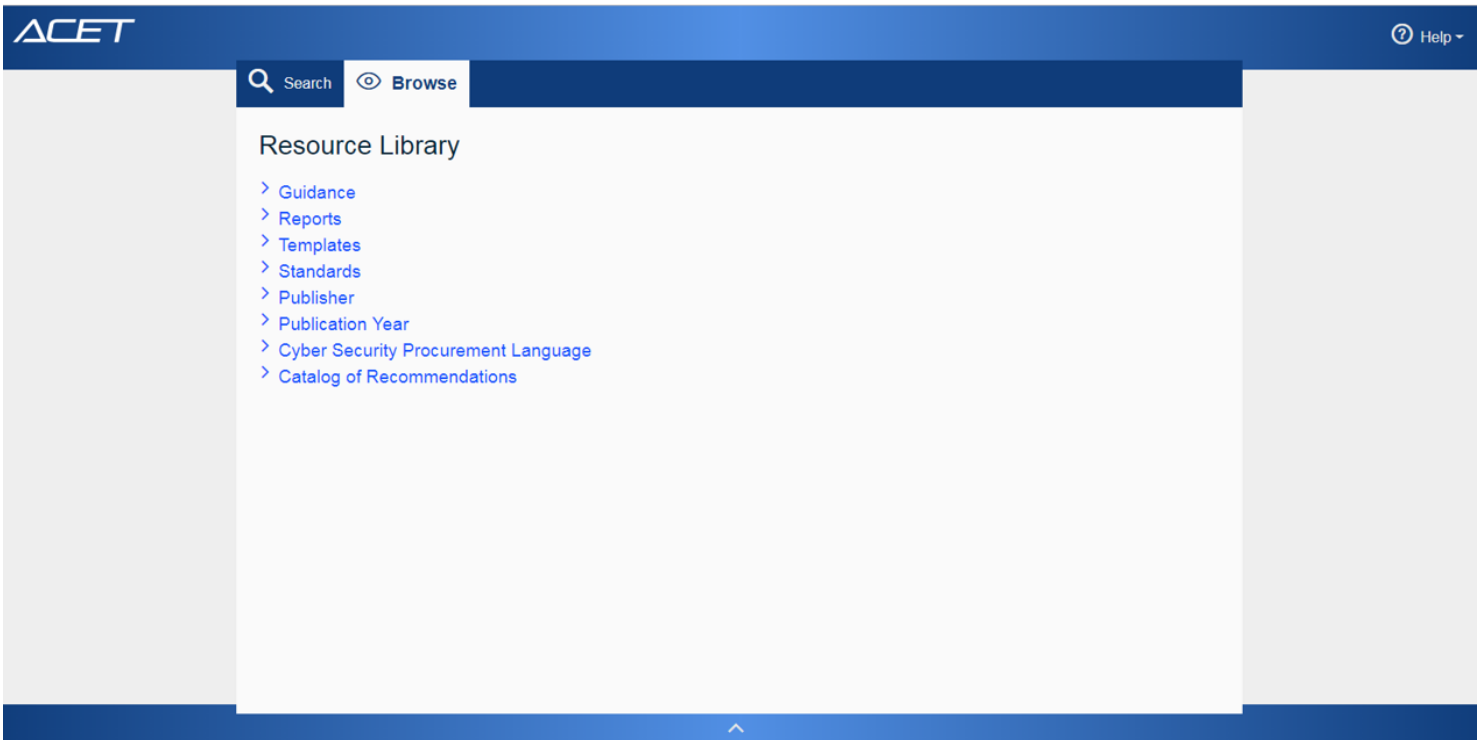


Figure: Resource Library Document Tree

Document Tree List: The Document Tree list displays the documents in the Resource Library organized by category in an expandable tree structure. The tree structure contains branches (Categories) and Leaves (Documents). Branches can be clicked to show more branches or leaves. Leaves can be clicked to display selected documents in a new tab.

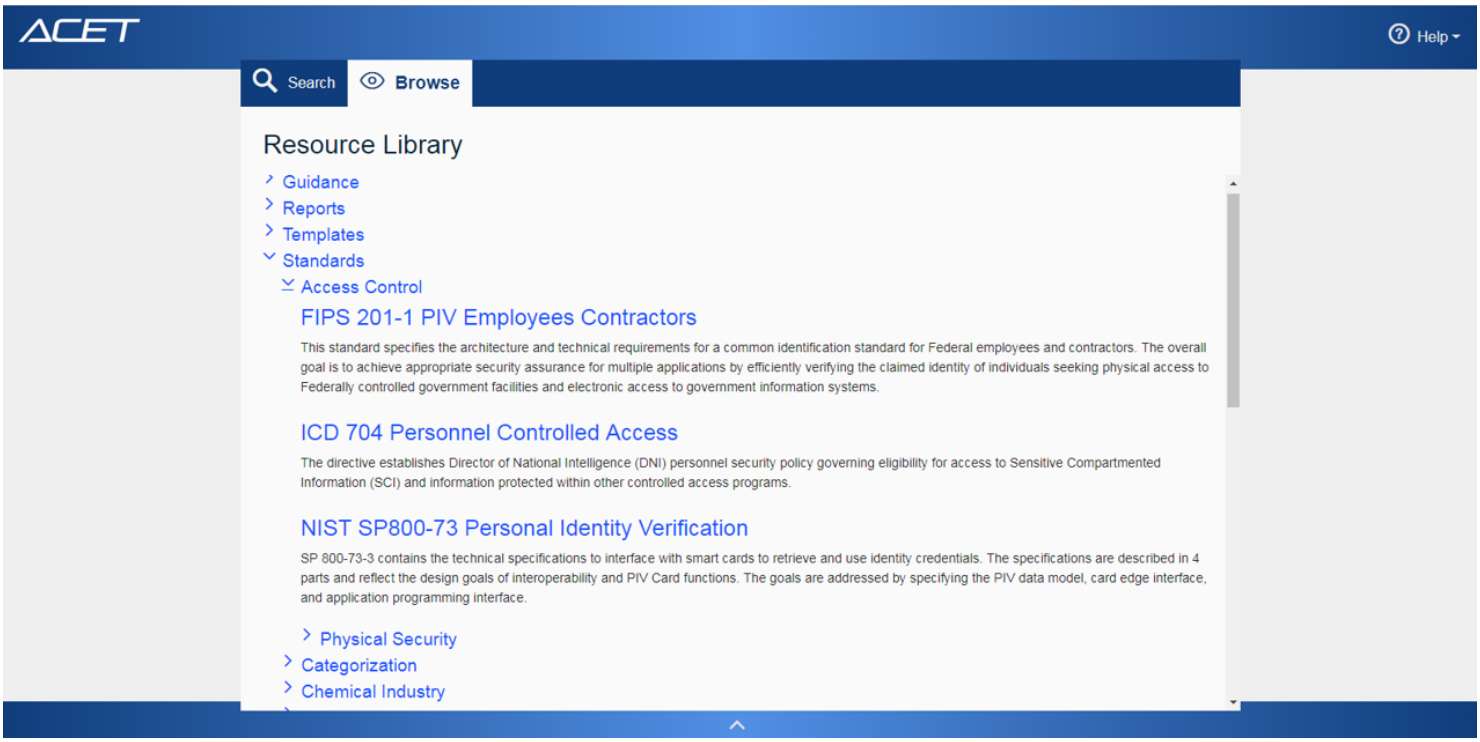


Figure: Expanded Document Tree

In the example shown in the figure above, the Access Control branch under Standards was clicked to open and expose the documents that are found under it. Any document selected will open in a new tab for the user to read.

The options to browse by publisher and publication year are also available. They were added for those users looking for specific versions of documents or documents from a specific source. The documents listed under these headings are the same as in the rest of the tree but listed in a differing order.

The final two subjects in the tree labeled Cyber Security Procurement Language and Catalog of Recommendations are unique and will open special access to the content rather than the files themselves.

Cyber Security Procurement Language:

By clicking the branch labeled Cyber Security Procurement Language, the screen expands the tree to show the topics in the Procurement Language document. (The full document can be found using the Search or Document Tree methods.) The figure below shows the branch open with the topic Removal of Unnecessary Services and Programs displayed (found under the System Hardening category.

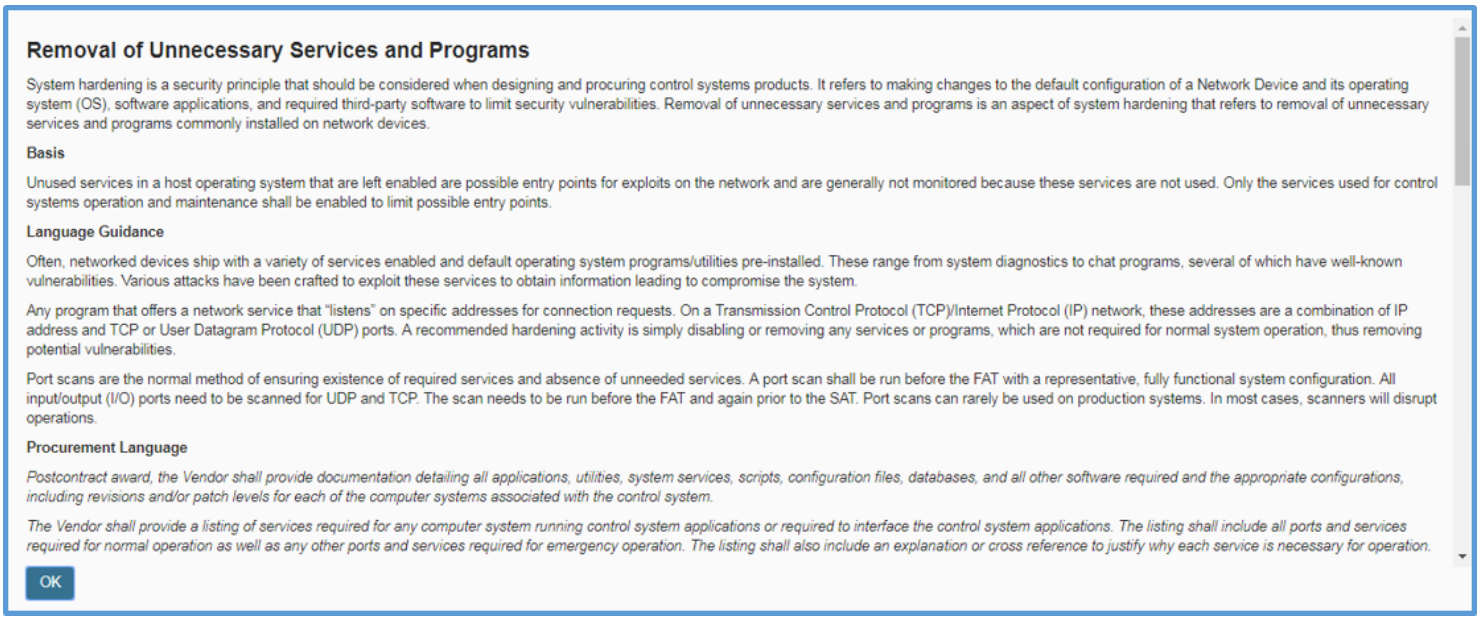


Figure: Cyber Security Procurement Language

In this case, instead of a document being opened, ACET displays formatted text taken directly from the Cyber Security Procurement Language document.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Basis,
- Language Guidance,
- Procurement Language,
- Factory Acceptance Test (FAT) Measures,
- Site Acceptance Test (SAT) Measures,
- Maintenance Guidance,
- Dependencies, and
- References.

To fully understand how the procurement language was developed, how it is to be used, any limitations and constraints, and general information about the document, open the document and read the front pages. To access it, click on Search and then type in procurement language.

Catalog of Recommendations:

This first level branch will open the list of topics that are associated with the Catalog of Control Systems Security: Recommendations for Standards Developers. The figure below shows an example.

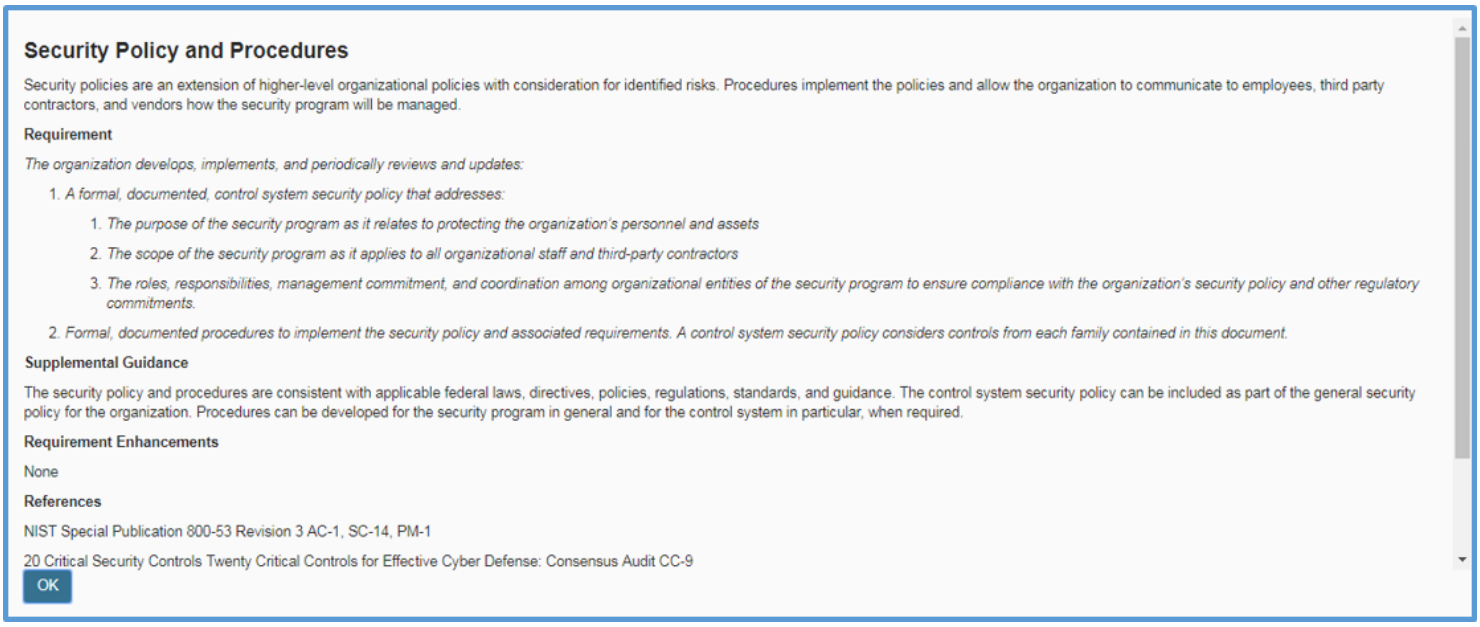


Figure: Catalog of Recommendations

Development of the Catalog was originally sponsored by DHS with input from NIST and five national laboratories. It consolidated the requirements from 15 control system and information technology Standards and was intended to serve as a source of requirements and controls for the developers of ICS Standards. Because of its popularity and comprehensive ICS requirements, it has become a principal Standard in all versions of ACET and in the ICS community at large in addition to Standards developers.

To access a topic, simply click on the branch title in the tree. In the example above, Security Policy was selected and the topic Security Policy and Procedures was chosen.

On the right-hand side of the screen, ACET displays the content from the Catalog.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Requirement Text,
- Supplemental Guidance,
- Requirement Enhancements, and
- References.

Like the procurement language document, to fully understand the background and intent of the Catalog, open and read the front pages.

User Profile

The User Profile menu allows the user to view their User Profile Information and their assessments, Change Password, and Logout of ACET.

The "My Assessments" link will navigate the user to their landing page. To learn more about the landing page, see ACET Landing Page.

The "Logout" link will log the user out and return them to the ACET home page.

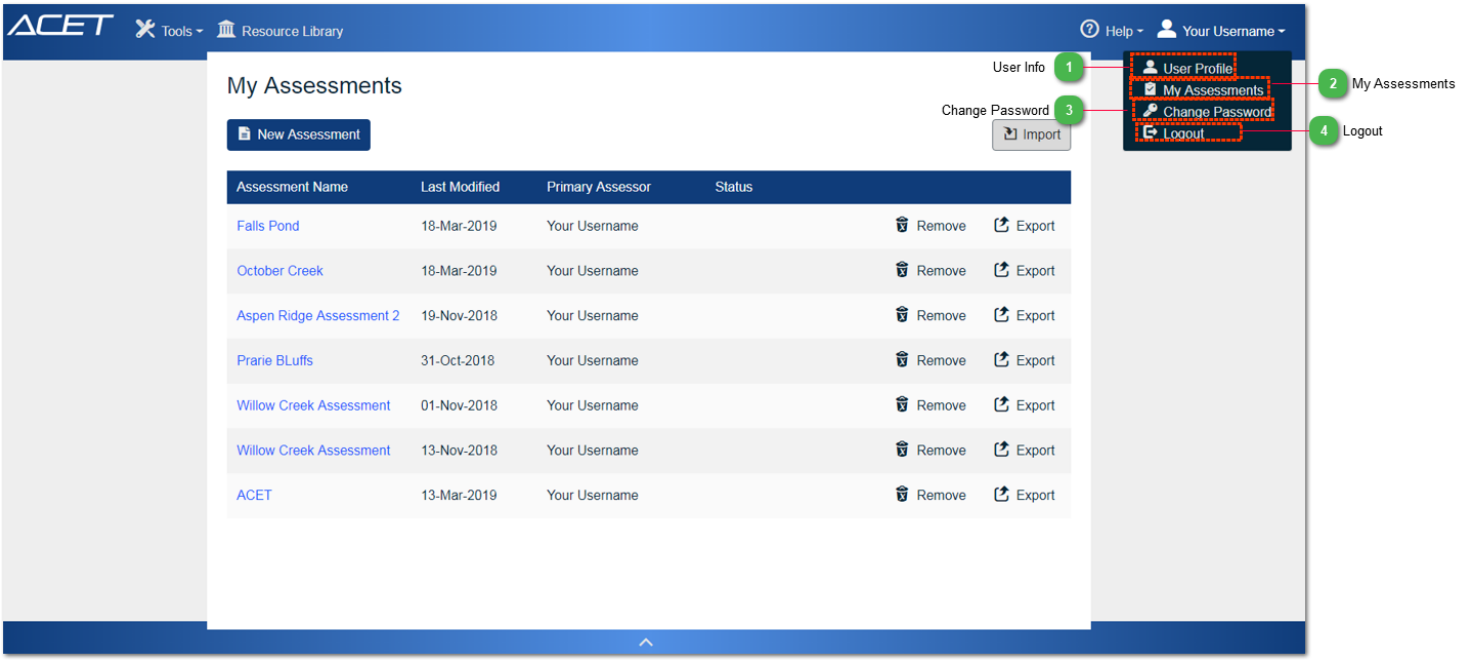


Figure: User Profile menu

1 User Info

User Profile

Click User Profile to view and edit User Profile Information.

See User Profile Information for more information.

2 My Assessments

My Assessments

Click My Assessments to be directed to the user's Landing Page.

See ACET Landing Page for more information.

3 Change Password

Change Password

Click Change Password to change the user's password.

See Change Password for more information.

4 Logout

Click Logout to be logged out of ACET and returned to the Home Page.

NOTE: When using the stand-alone version of ACET the only option available in the User Profile menu is "My Assessments". The User Profile menu will always be labeled "Local User".

User Profile

The User Profile menu allows the user to change their First Name, Last Name, and/or Email. The menu also provides a space for the user to choose and enter answers for security questions.

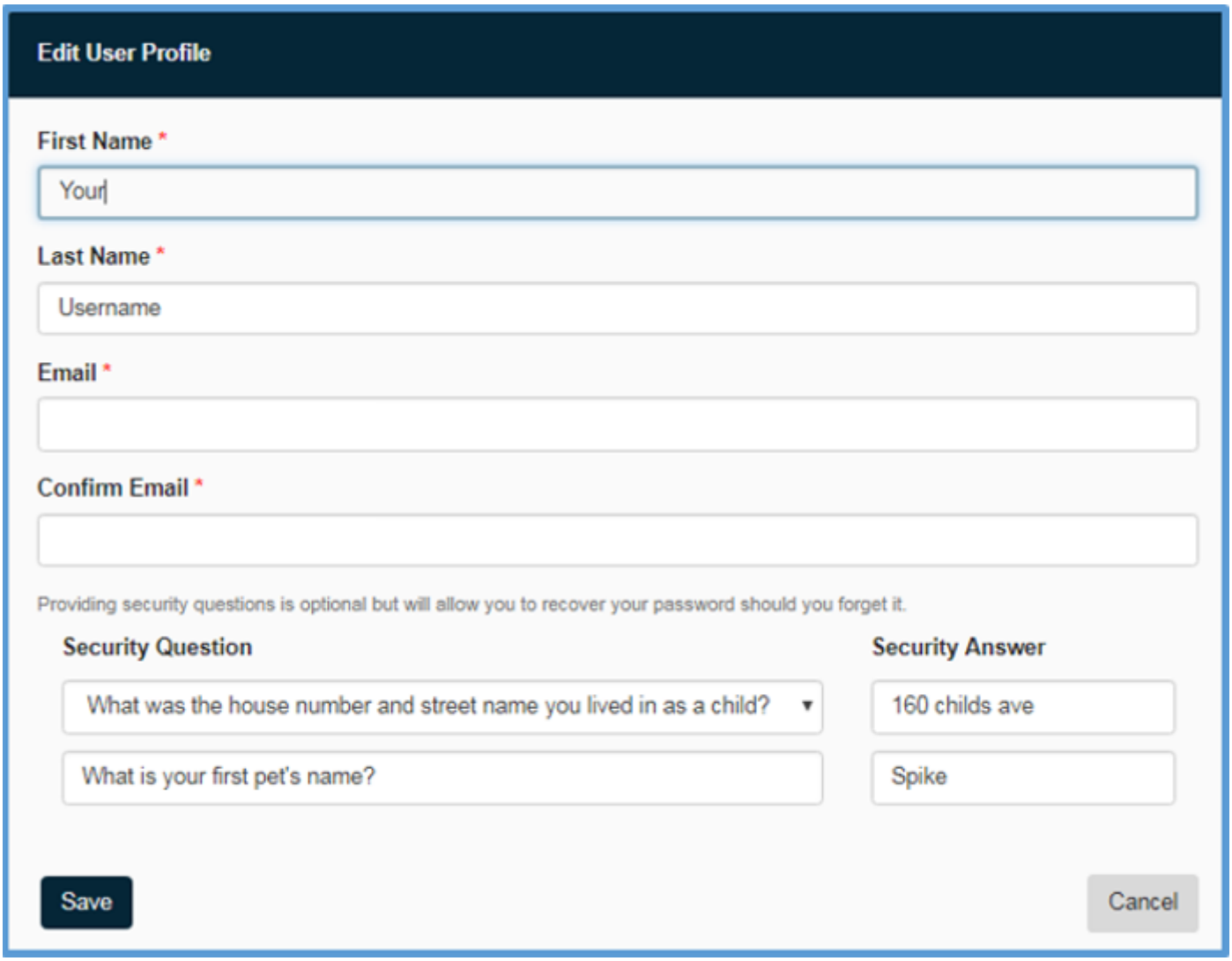


Figure: Edit User Profile dialogue

The User Profile dialogue will show your profile information. Use this dialogue to change first and last name or email. Select the "Save" button to keep changes or "Cancel" to exit the dialogue.

Select a Security Question from the dropdown and type your answer in the Security Answer field. These questions will be used if you forget your password.

Change Password

Users can select the "Change Password" link to change their password.

Enter the Current Password and New Password twice to change passwords.

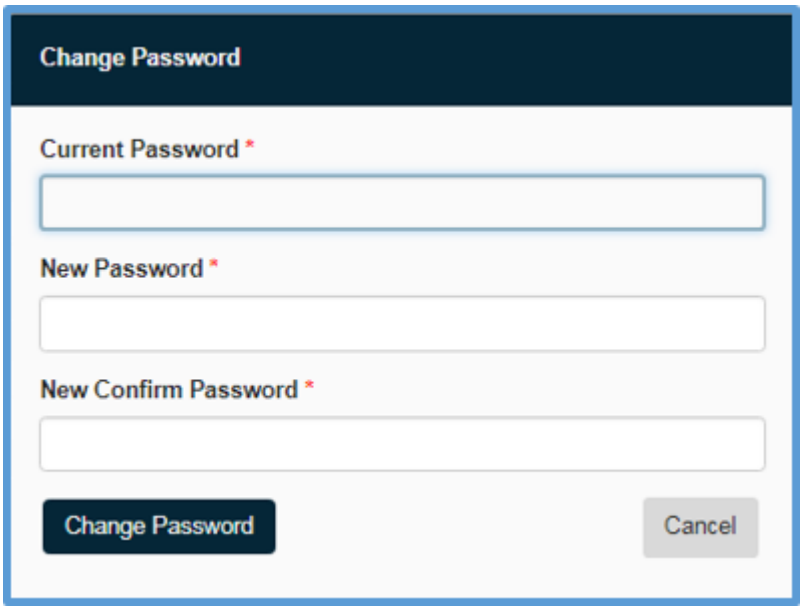


Figure: Change Password dialogue

Help Menu

The Help Menu shown in the figure below allows the user to access help documentation for the ACET tool.

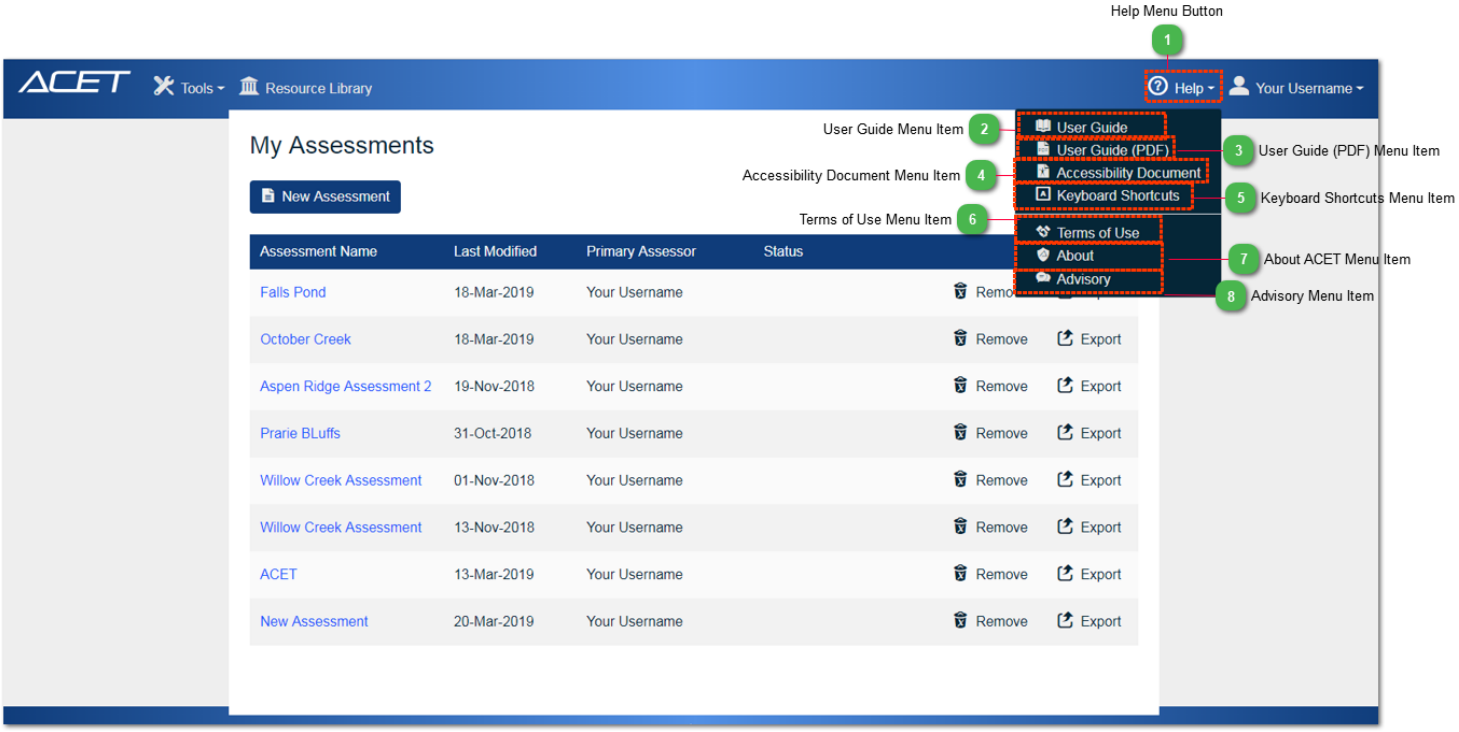


Figure: Help Menu

1 Help Menu Button

Clicking the Help menu button opens the Help menu.

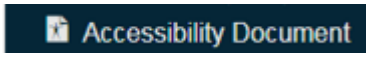
2 User Guide Menu Item

Clicking the User Guide menu item will open this user guide as a CHM file containing screen shots and instructional information for using the ACET tool.

3 User Guide (PDF) Menu Item

Clicking the User Guide (PDF) menu item will open this user guide as a PDF file containing screen shots and instructional information for using the ACET tool.

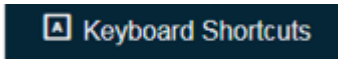
4 Accessibility Document Menu Item



Clicking the Accessibility Document menu item will open the ACET Accessibility Features Document, which describes how ACET addresses accessibility issues including the use of high contrast mode, and keyboard access.

See Accessibility Document for more information.

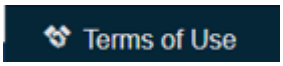
5 Keyboard Shortcuts Menu Item



Clicking the Keyboard Shortcuts menu item will open the ACET Keyboard Shortcuts document, which contains a list of all keyboard shortcuts available to users of the ACET tool.

See Keyboard Shortcuts for more information.

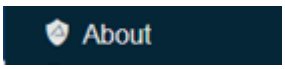
6 Terms of Use Menu Item



Clicking the Terms of Use menu item will open the ACET Terms of Use that describes the terms that user's agree to when using ACET.

See Terms of Use for more information.

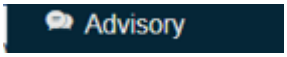
7 About ACET Menu Item



Clicking the About ACET menu item will open the About ACET window containing version information, web site links to videos, training and contact information for the ACET team.

See About ACET for more information.

8 Advisory Menu Item

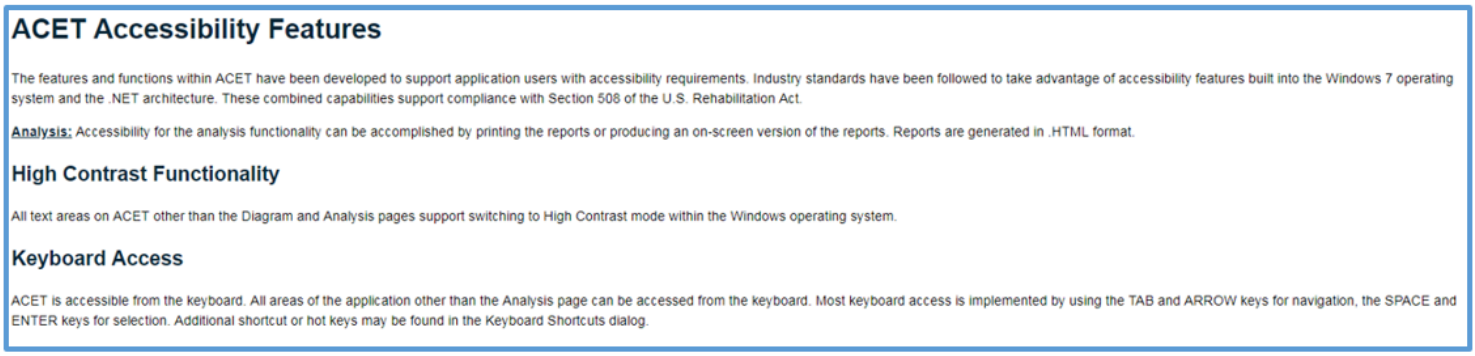


Clicking the Advisory menu item will open the Advisory window that contains disclaimer information.

See Advisory for more information.

ACET Accessibility Features

The figure below shows the ACET Accessibility Features document that can be accessed from the Help menu of the ACET tool.



ACET Accessibility Features

The features and functions within ACET have been developed to support application users with accessibility requirements. Industry standards have been followed to take advantage of accessibility features built into the Windows 7 operating system and the .NET architecture. These combined capabilities support compliance with Section 508 of the U.S. Rehabilitation Act.

Analysis: Accessibility for the analysis functionality can be accomplished by printing the reports or producing an on-screen version of the reports. Reports are generated in .HTML format.

High Contrast Functionality

All text areas on ACET other than the Diagram and Analysis pages support switching to High Contrast mode within the Windows operating system.

Keyboard Access

ACET is accessible from the keyboard. All areas of the application other than the Analysis page can be accessed from the keyboard. Most keyboard access is implemented by using the TAB and ARROW keys for navigation, the SPACE and ENTER keys for selection. Additional shortcut or hot keys may be found in the Keyboard Shortcuts dialog.

Figure: ACET Accessibility Features Document

Keyboard Shortcuts

The figure below shows the ACET Keyboard Shortcuts document that can be accessed from the Help menu of the ACET tool.

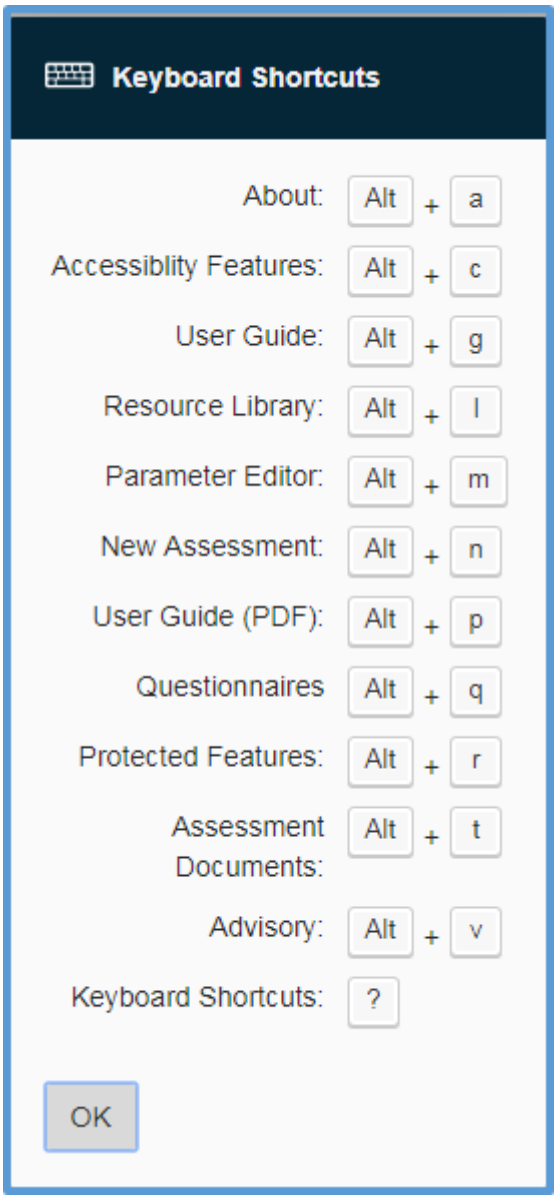


Figure: ACET Keyboard Shortcuts Document

Terms of Use

The figure below shows the Terms of Use that can be accessed from the Help Menu.

Figure: Terms of Use

About ACET

The About ACET window provides the user with more information about the ACET team. It includes contact information, version number, and training information.

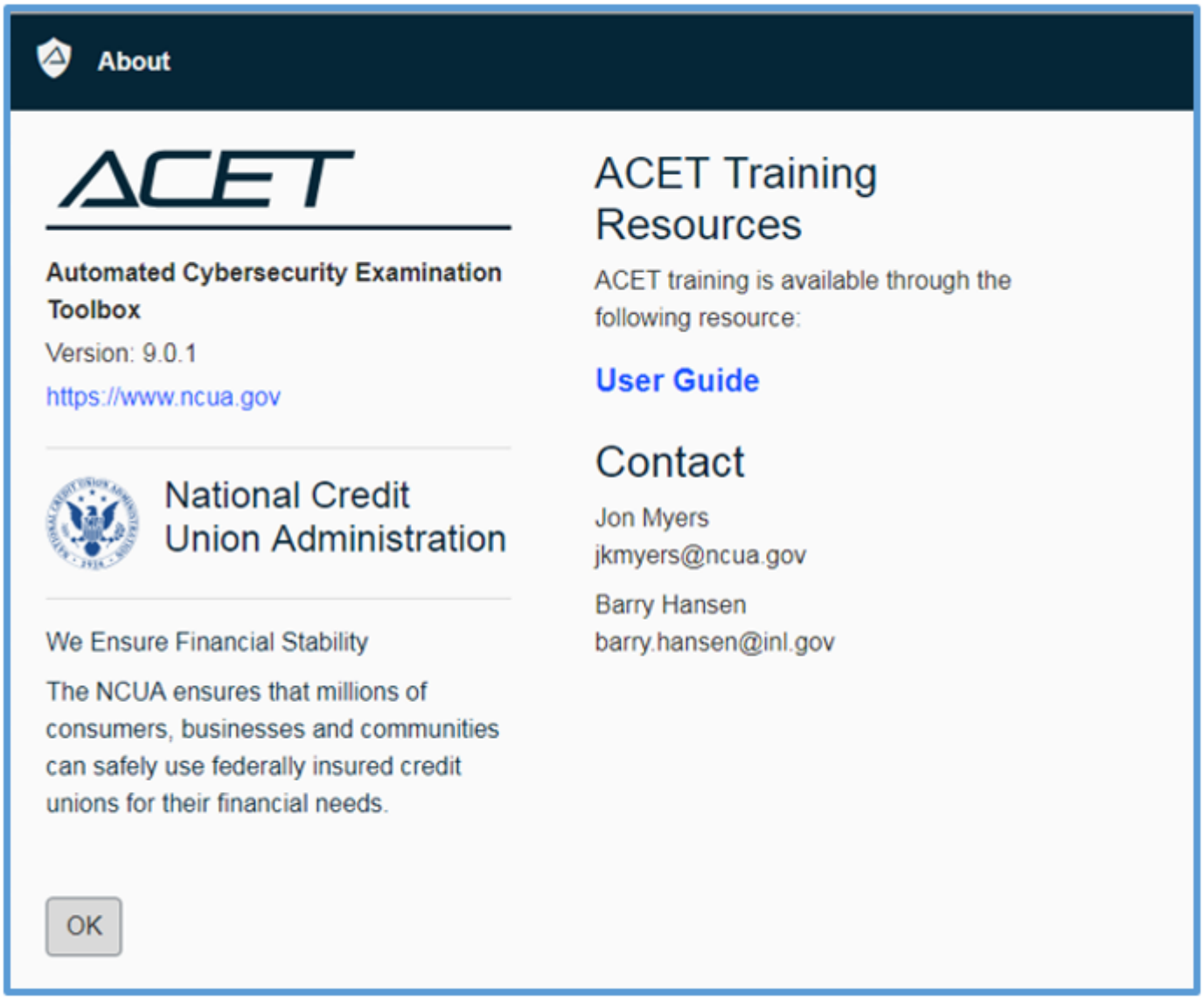


Figure: About ACET Window

Advisory

The figure below shows the Advisory window that can be accessed from the Help menu of the ACET tool.

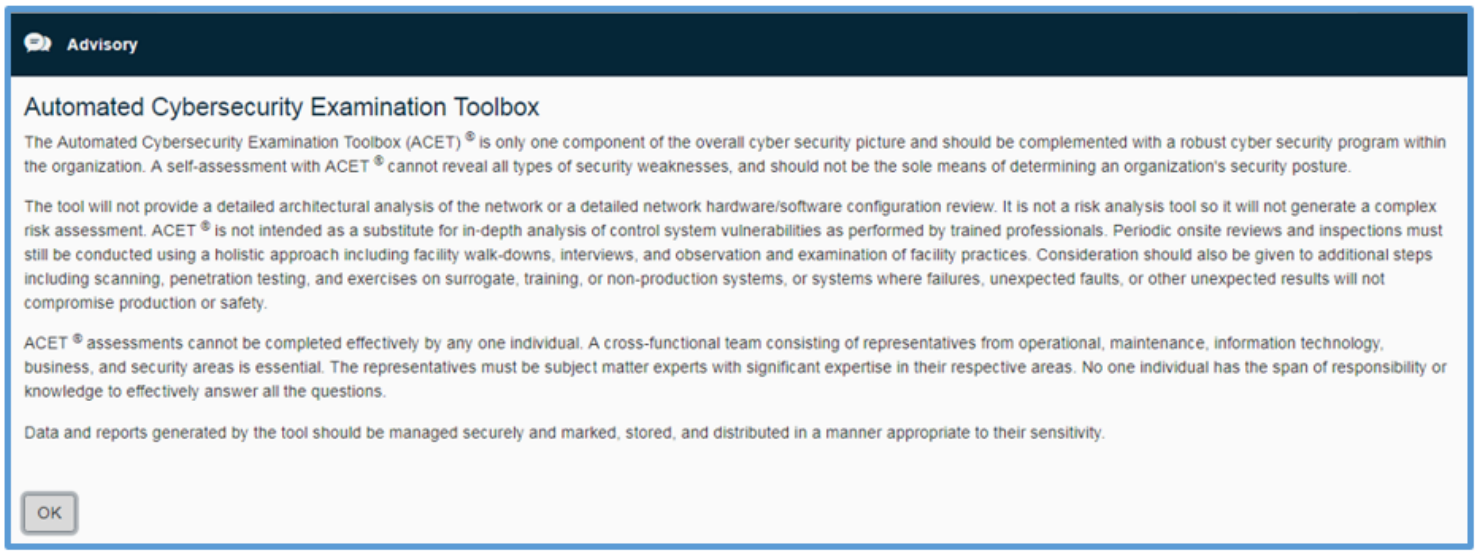


Figure: Advisory Screen

Operation Menus

This section addresses the main operation menus of the ACET assessment tool. They include the Prepare Menu, the Assessment menu, and the Results menu.

Prepare Menu

The Prepare menu allows quick access to the assessment prepare screens. The figure below describes the buttons and menu.

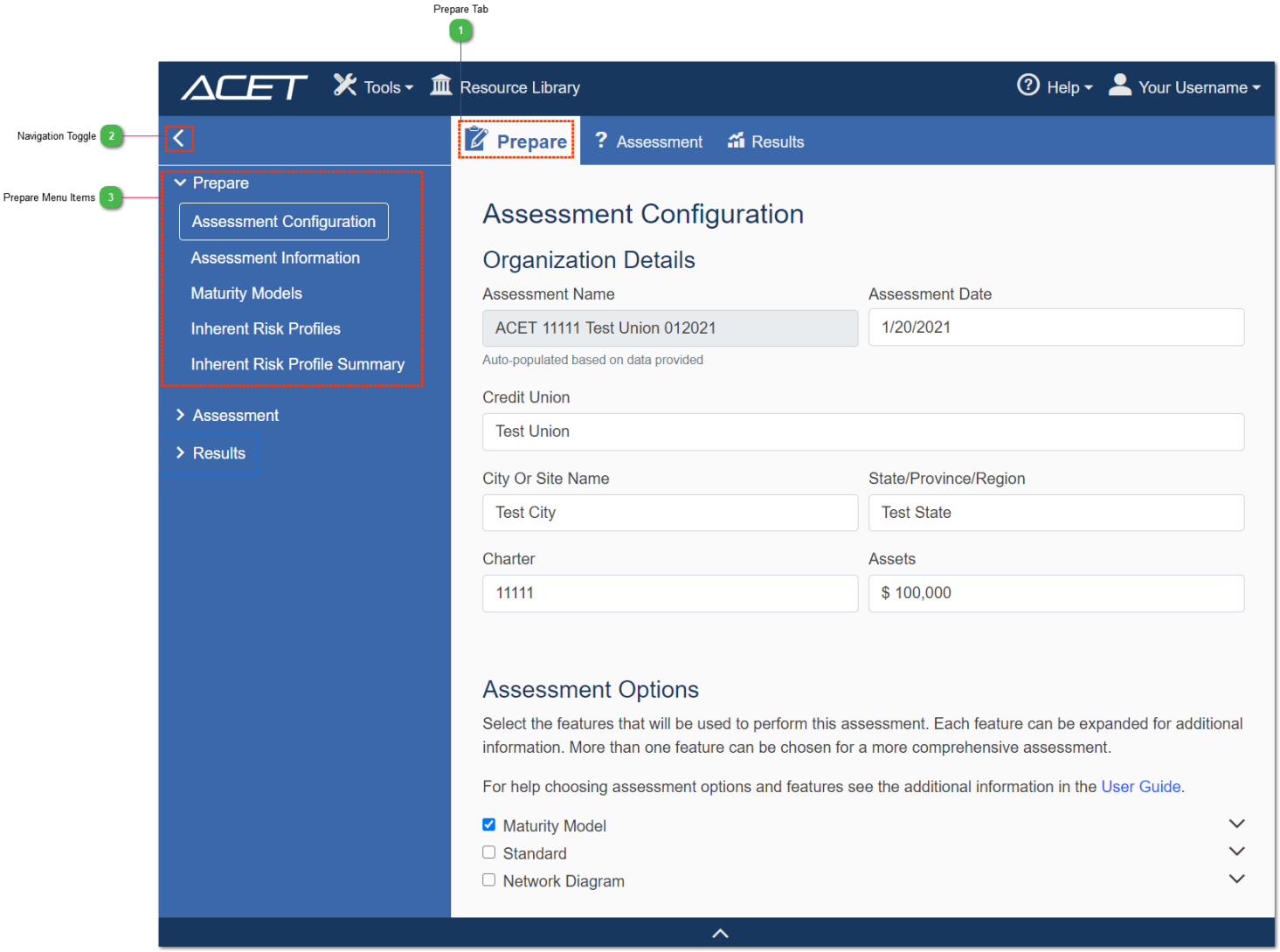


Figure: Prepare Button/Menu

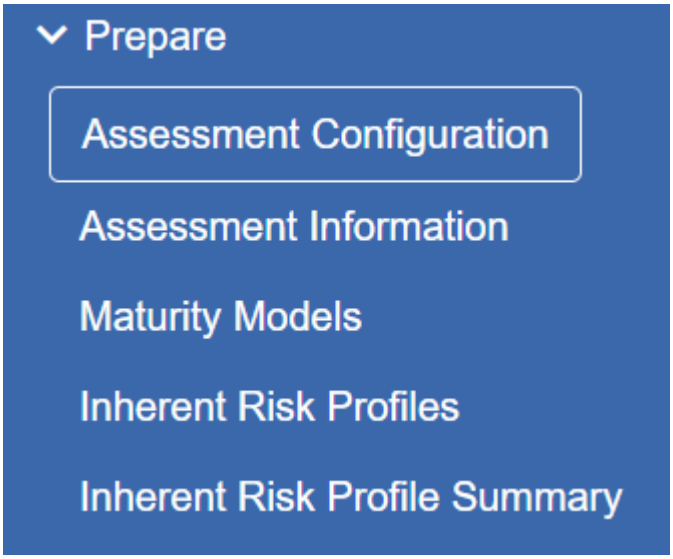
1 Prepare Tab

Clicking the Prepare button will display the Assessment Configuration screen.

2 Navigation Toggle

Use the Navigation Toggle to open and close the Navigation Menu.

3 Prepare Menu Items



The Prepare menu items indicate the screens encountered by the user during the preparation process.

See Assessment Configuration, Assessment Information, Inherent Risk Profiles, and Inherent Risk Summary for more information.

Statements Menu

The Statements menu allows quick access to the assessment statements and categories. The figure below shows the Statements menu navigation. In ACET only mode the only option available is the Statements tab. To use the Question/Requirements tabs uncheck ACET only mode. See more in the Assessment Information section.

NOTE: Requirements mode navigation will differ in that it shows standards at the top level and then categories nested underneath them.

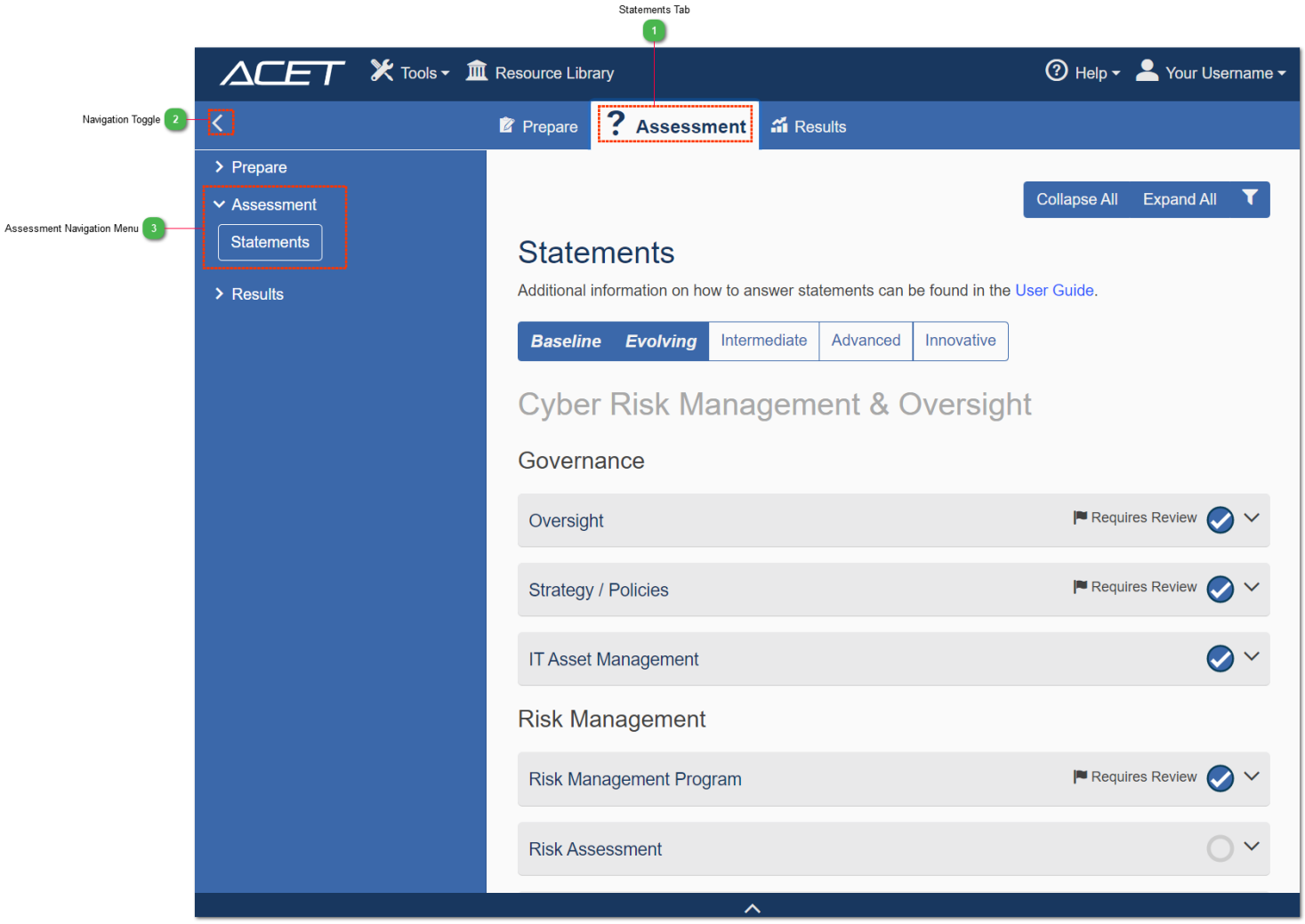
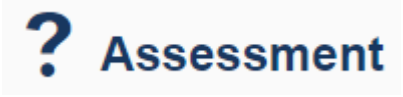


Figure: Assessment Button/Menu

1 Statements Tab



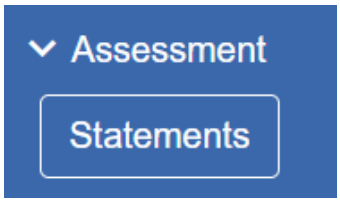
Clicking the Assessment Tab will display the Statements screen displayed after the Prepare process.

See the Assessment Section for more information about the Statements screen.

2 Navigation Toggle

Use the Navigation Toggle to open and close the Navigation Menu.

3 Assessment Navigation Menu



The Assessment Navigation menu shows a list of all statement categories awaiting completion for the assessment.

Results Menu

The Results menu allows quick access to the assessment results and reports screens. The figure below shows the Results menu.

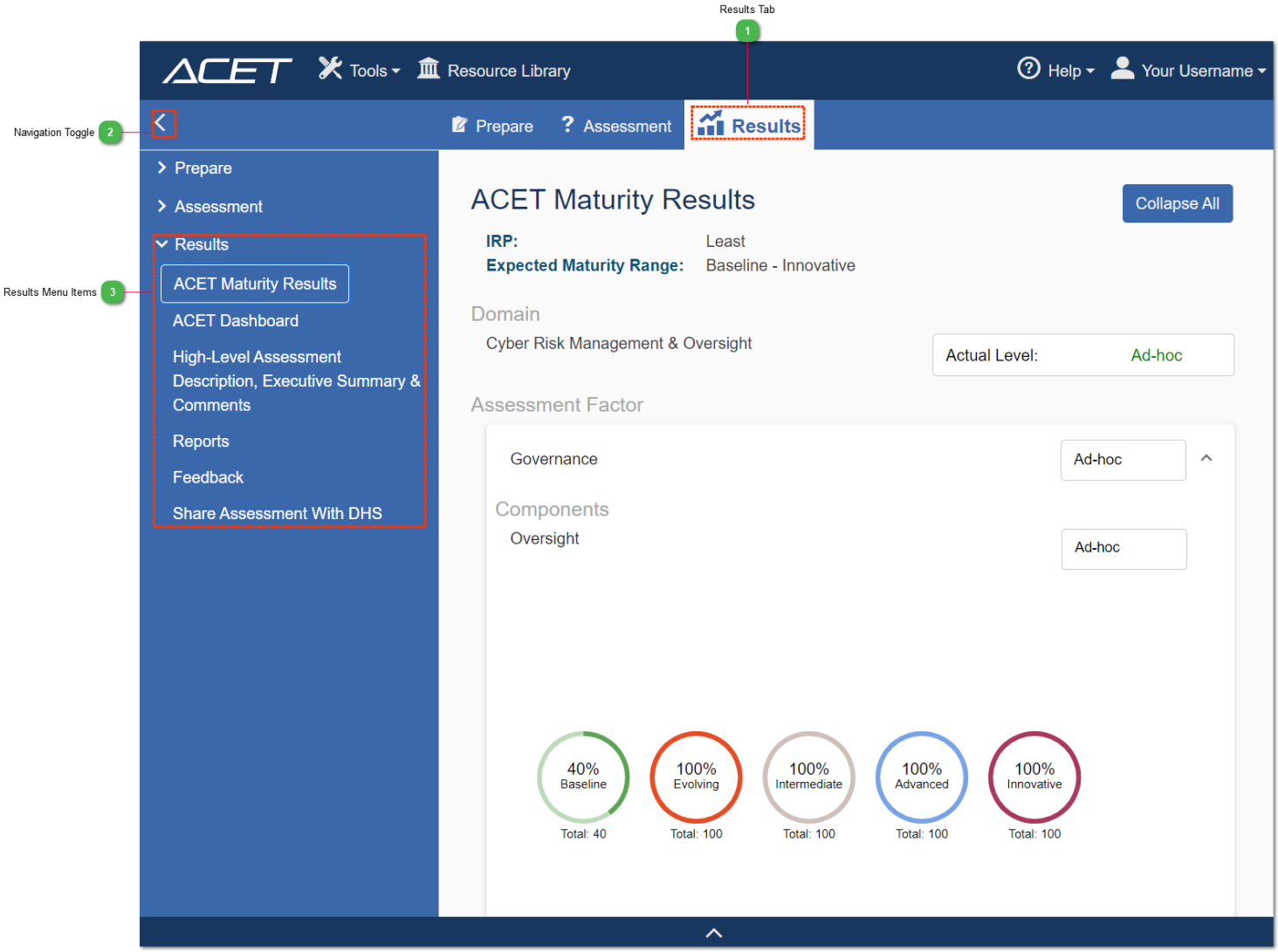


Figure: Results Button/Menu

1 Results Tab

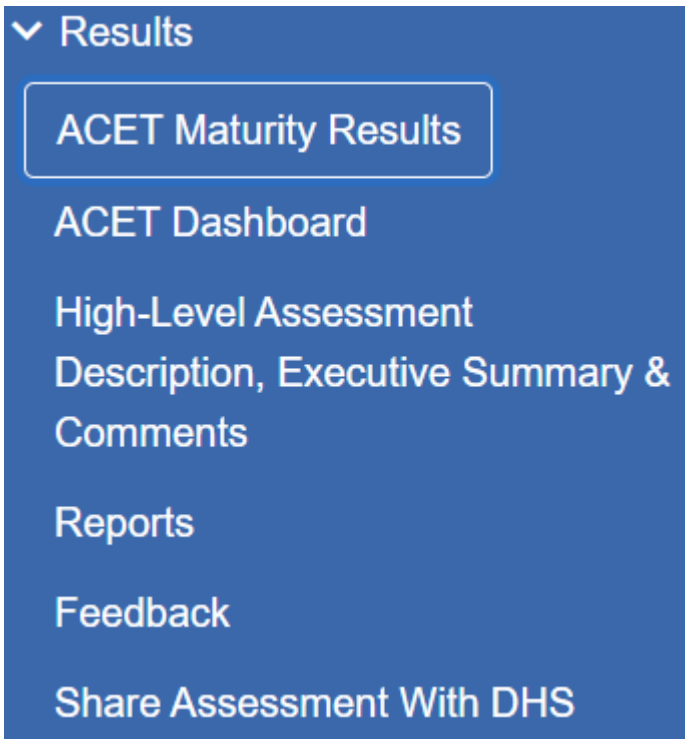
Clicking the Results button will display the Results Overview screen.

See the Results Menu for more information.

2 Navigation Toggle

Use the Navigation Toggle to open and close the Navigation Menu.

3 Results Menu Items



The Results menu items indicate the screens available to the user in the main Results Section.

Main ACET Window Sections

This part of the user manual contains information about the different sections of the main ACET window including the Preparation, Assessment, and Results sections.

Prepare Section

The Prepare section is where the assessment process begins. The preparation screens help the user to quickly get ready to answer the appropriate questions for their facility by defining the questions that will be answered during the assessment. The following pages will describe the preparation screens in more detail.

ACET Landing Page

The ACET Landing page is the first screen seen after logging in. The figure below shows the ACET Landing Page.

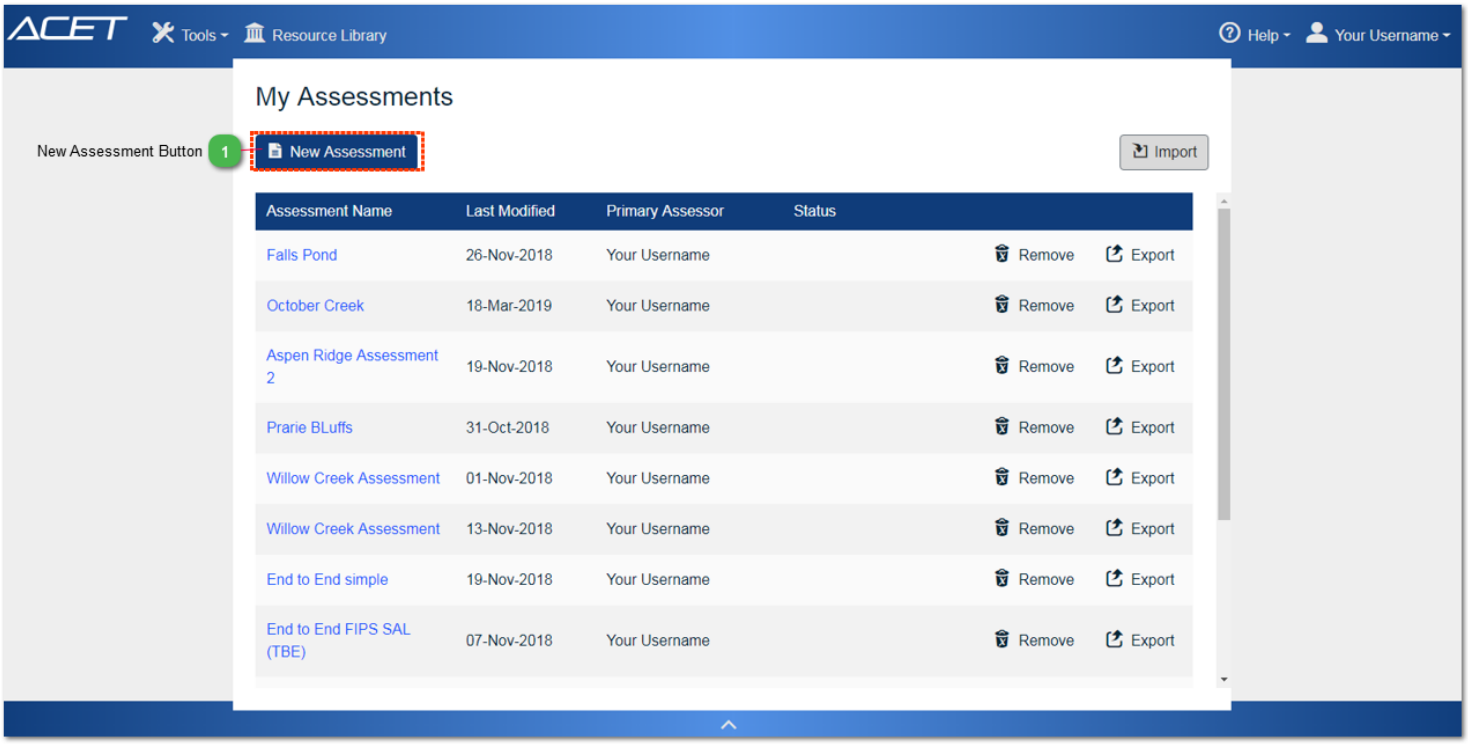


Figure: ACET Landing Page

1 New Assessment Button

Clicking the New Assessment button will start the assessment preparation process that will allow the user to address important areas before they can begin answering questions.

The first screen of the assessment preparation process is the Assessment Details screen.

Tip: All the Landing page columns can be sorted by clicking the arrow next to the column name.

Assessment Configuration

Clicking the Assessment Configuration menu item in the Prepare Menu opens the Assessment Configuration screen. This screen allows for collecting specific information about the assessment including when it occurred, what credit unions were involved, and both descriptive and summary information. To use the Assessment Configuration screen, simply enter textual data into the fields provided. The figure below addresses the different parts of the Assessment Configuration screen.

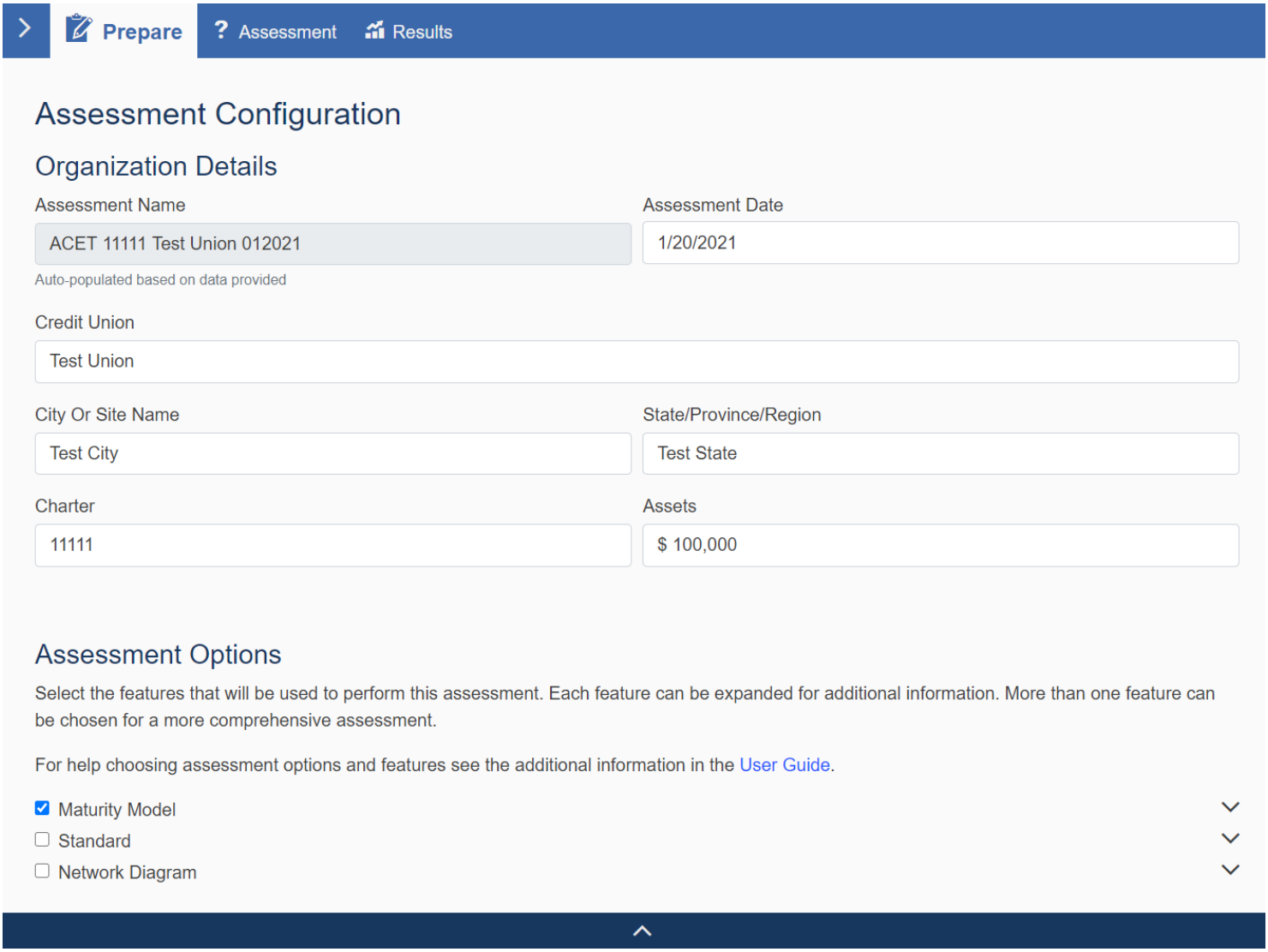


Figure: Assessment Configuration screen

Assessment Name: The Assessment Name field populates based on the charter number, credit union name, and assessment date. This field isn't editable itself. Changes must be made within the charter, credit union, and assessment date fields to update the name.

Assessment Date: The Assessment datepicker enables a user to add an initial date for the assessment. It requires a valid date format. Clicking the calendar icon will allow the user to select a date from a calendar control rather than entering the date manually.

Credit Union: The Credit Union text box is where the user enters the Credit Union for which the assessment is being completed.

City/Site and State/Province/Region: The Location text boxes provide text input for identifying the name of the City or Site for which the assessment is created as well as the State, Province, or Region for which the assessment is created.

Charter: The Charter box is where the user enters their charter number. Only numbers are accepted in this field.

Assets: The Assets box is where the user enters the dollar amount of assets the Credit Union has.

Assessment Options

There are three different features for building an assessment. You can select one or more.

Maturity Model: A maturity model is a formal measurement used by an organization to gauge and improve its programs and processes. Maturity models are intended to measure the degree to which an organization has institutionalized its cybersecurity practices. Implementing process maturity within an organization will ensure that practices are consistent, repeatable, and constantly being improved.

NOTE: ACET is a maturity model and is available in the Maturity Model Selection page.

Standard: An ACET cybersecurity assessment examines the organization's cybersecurity posture against a specific standard. The assessment tests its security controls and measures how they stack up against known vulnerabilities.

Network Diagram: A network diagram is a visual representation of a computer or network. It shows the components and how they interact, including routers, devices, hubs, firewalls, etc. and can help define the scope of the network for the assessment.

Assessment Information

Contacts Management

Contacts Management is handled within the Assessment Information screen.

Figure: Contacts Management panel

The Contacts panel shows first shows the Assessment Owner's name and below that will be their email address. This is the user who created the assessment.

To add a contact click the "Add Contact" button.

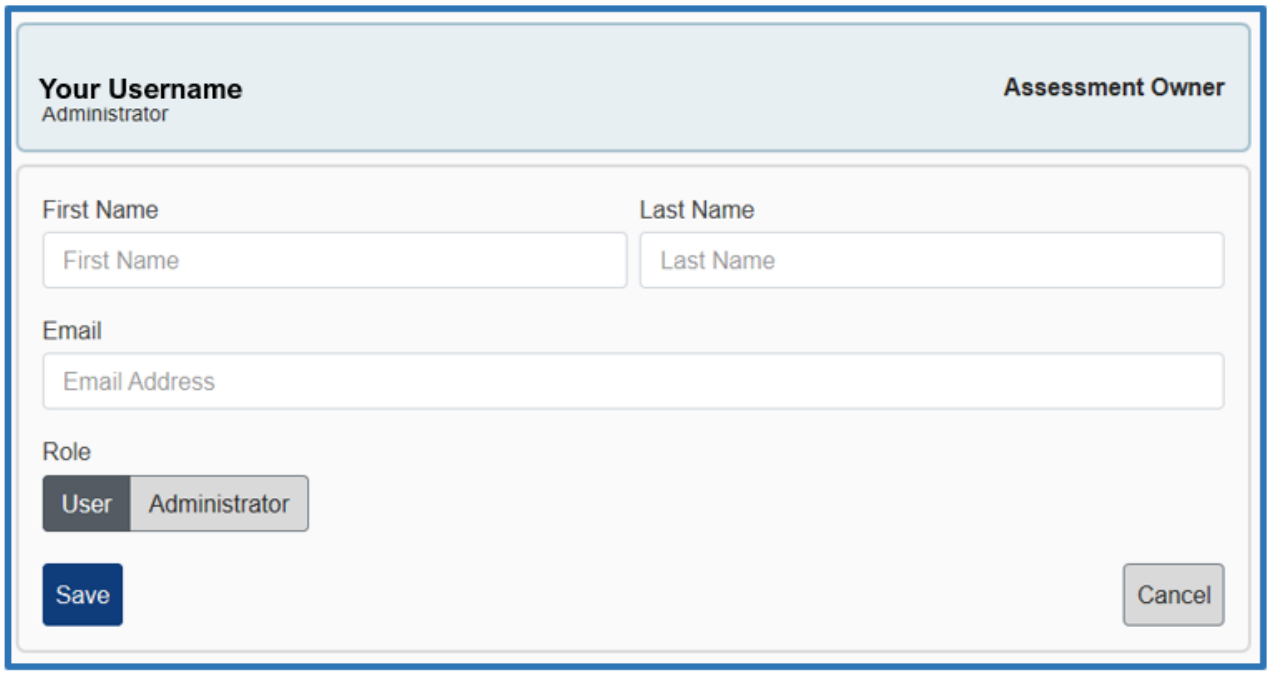


Figure: Add a New Contact

Add a New Contact: After selecting "Add Contact" a dialogue will open up below. Add the contacts information in the First Name, Last Name, and Email fields. If the contact has been previously associated with the user then the fields will auto-populate.

Select the User or Administrator role toggle. Administrators can add and remove contacts to an assessment, and delete assessments. There must be an Administrator assigned to an assessment at all times.

Select Save or Cancel to exit the dialogue.

When a user is added to an assessment they are sent an email inviting them to that ACET assessment. If they haven't yet registered for a ACET account they will be sent an additional email to walk them through the registration process.

Figure: Added user to assessment and contact icons

Editing a Contact: Clicking the Change icon 

makes the contact text field editable so that changes can be made. Click the save button to commit changes.

Removing a Contact: Clicking the Remove icon 

allows the user to delete contacts from an assessment. A confirmation dialogue will come up.

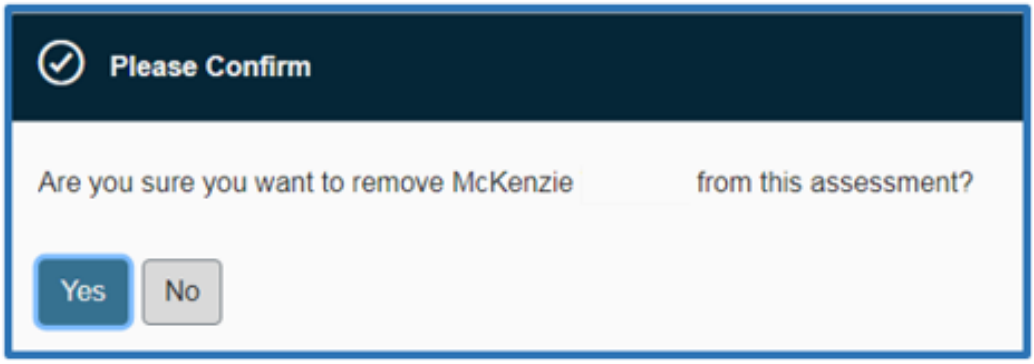


Figure. Contact Deletion dialogue

Selecting "Yes" will remove the contact from the assessment. Selecting "No" will keep the user associated with the assessment.

Maturity Models

The Maturity Model page is where you will select which model you'd like to base your assessment on.

Figure: Maturity Model page

ACET is pre-selected. Currently there are three maturity models: CMMC, EDM, and ACET. See...for more information...

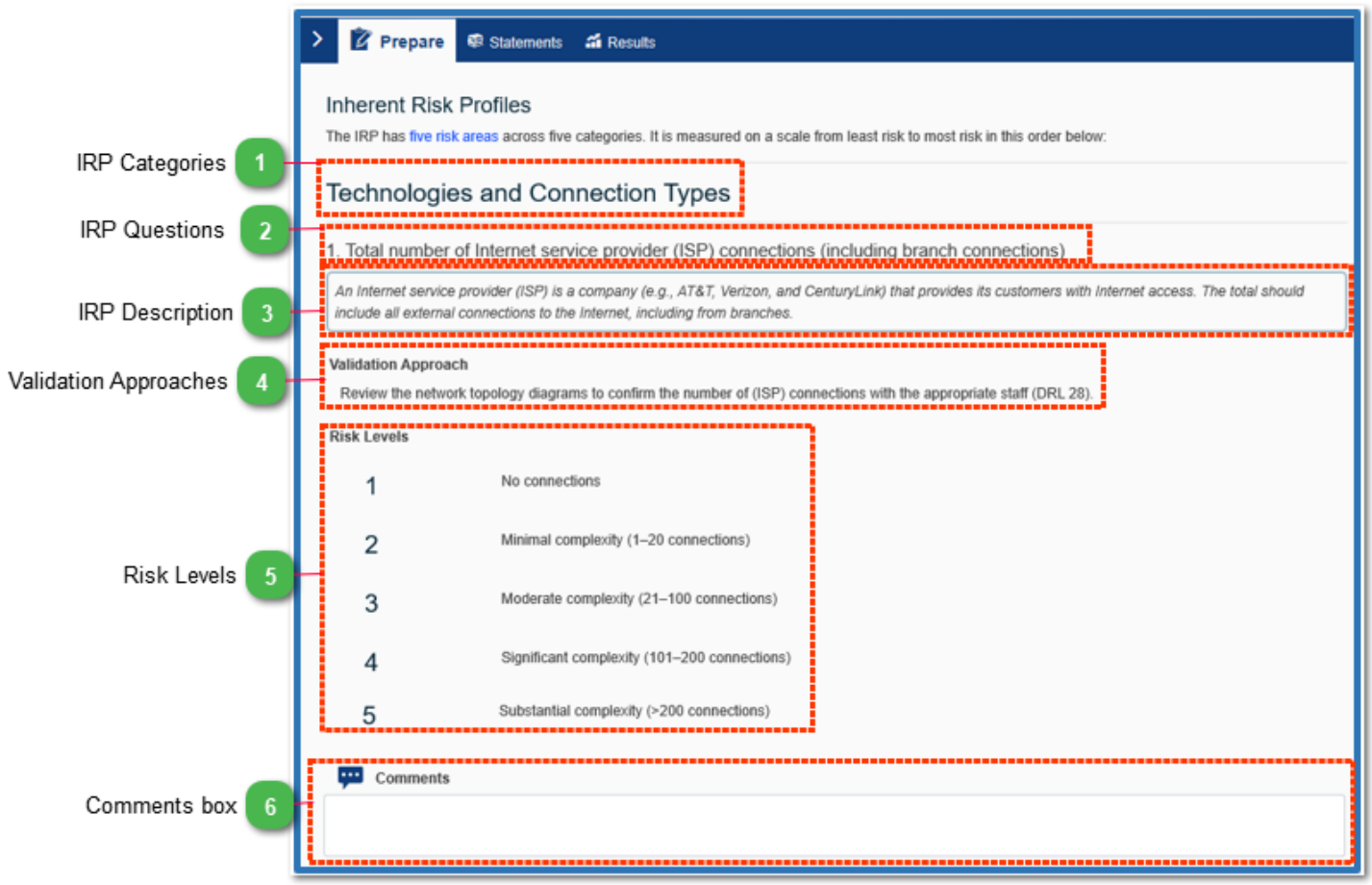
Only one maturity model can be selected at a time.

Inherent Risk Profiles

The Inherent Risk Profile (IRP) has five risk areas across five categories. It is measured on a scale from least risk to most risk in this order below:
1. Least - very limited use of technology.
2. Minimal - limited complexity in terms of the technology it uses.
3. Moderate - uses technology that may be somewhat complex in terms of volume and sophistication.
4. Significant - uses complex technology in terms of scope and sophistication.
5. Most - uses extremely complex technology to deliver myriad products and services.

First, enter a response of 1-5 for all items on the IRP screen. Base responses on interviews with management and/or provided support documentation. Examiners cannot require credit unions to complete the ACET. If the credit union has completed the FFIEC CAT, use these results to assist in completing the ACET. There is often more than one way to verify responses. Therefore, each item provides potential verification approaches, rather than required examination steps.

An examiner reviews the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain in order to understand whether the risk and maturity are in alignment. Both IRP levels and Cybersecurity Maturity results can be seen in the ACET dashboard. For more information about the ACET dashboard, see the help section.



1 IRP Categories

Technologies and Connection Types

The IRP Categories break the IRP questions into groups.

2 IRP Questions

Users select Risk Levels for each individual IRP Question.

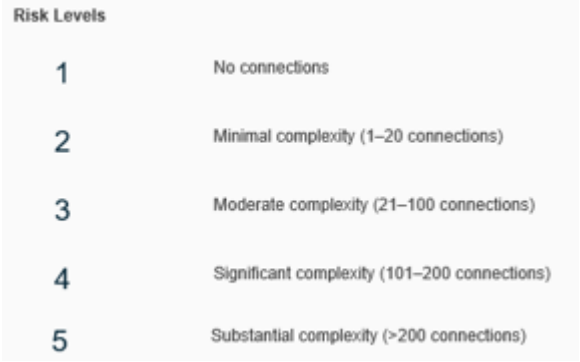
3 IRP Description

The IRP Description gives additional context to help the user determine a risk level.

4 Validation Approaches

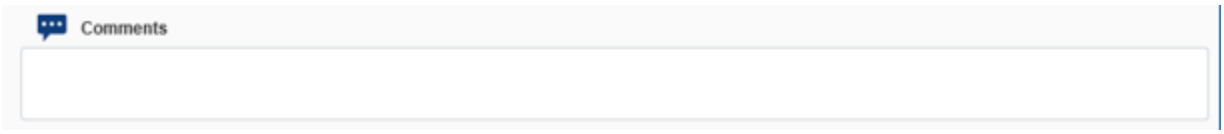
The Validation Approaches are suggestions, but not requirements. Examiners should consider materiality, reasonableness, and use professional judgement when determining the depth of verification necessary for a particular response.

5 Risk Levels



The Inherent Risk Profile (IRP) has five risk areas across five categories. It is measured on a scale from least risk to most risk in this order below:
1. Least - very limited use of technology.
2. Minimal - limited complexity in terms of the technology it uses.
3. Moderate - uses technology that may be somewhat complex in terms of volume and sophistication.
4. Significant - uses complex technology in terms of scope and sophistication.
5. Most - uses extremely complex technology to deliver myriad products and services.

6 Comments box



The comments box allows the user to leave a comment about the particular IRP question.

Inherent Risk Summary

The Inherent Risk Summary page displays the Inherent Risk levels for the questions users answered on the Inherent Risk Profiles page.

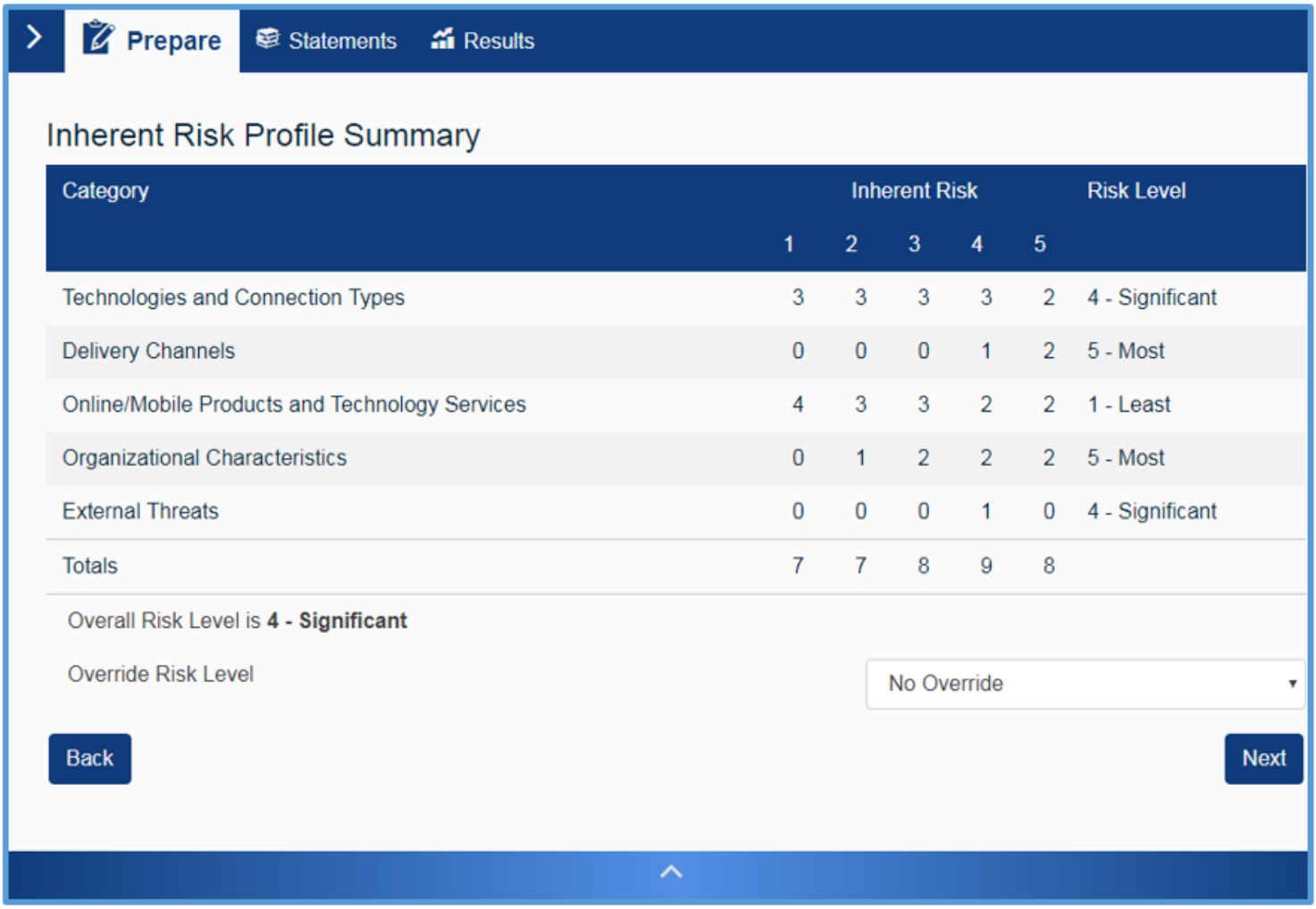


Figure: Inherent Risk Summary

Users can use the Total Risk Level Override dropdown to override their calculated Total IRP level. After selecting a new total IRP level the Override Reason comment field will open. Users are encouraged to provide a reason for IRP override.

Assessment Section

The assessment section is where the user answers questions related to the selected Standards or Profile and Security Assurance Level. The following sections will describe the Assessment process in detail.

Assessment Screen

The primary interaction that takes place in ACET happens on the Assessment screen. The Assessment screen displays statements for you to read and answer. The results of the combined answers to the presented statements will help to provide a good perspective and understanding of the organization's cybersecurity posture.

Completing the statements portion of the assessment is where most of the time will be spent. The process of answering statements is not difficult but it can be tedious. It's recommended to plan ahead and recognize that it will take several hours or even days to accurately answer all the questions. The more time spent understanding the intent of each question and then discussing it as a team, the more valuable the assessment will be. Take the time to fully understand the intent of each question then provide the answer that best meets the current situation. If upgrades are in progress at the time of the assessment, comments can be associated with the relevant questions to document the activity.

The figure below shows the main sections of the Assessment screen.

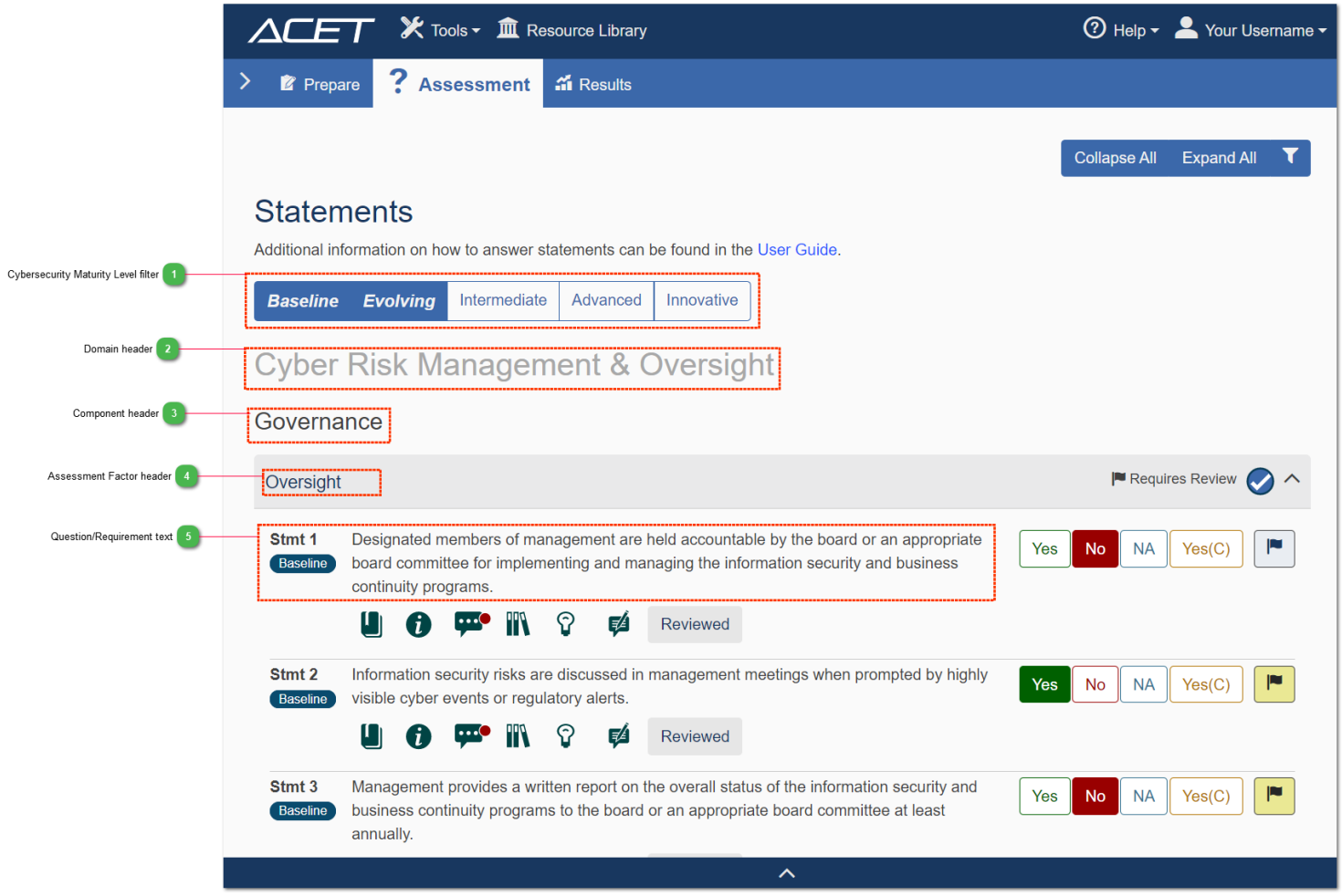
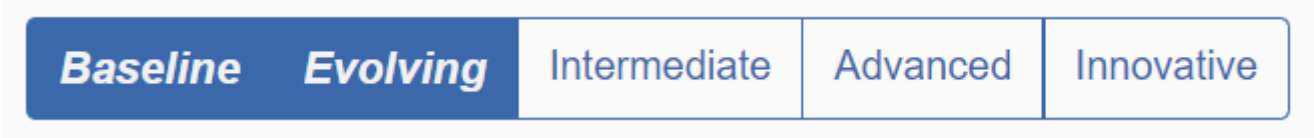


Figure: Assessment Screen

1 Cybersecurity Maturity Level filter



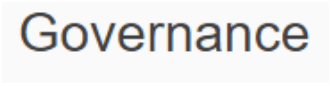
The filter shows in italics the levels that the user has been assigned and displays statements in those levels below. Users can change the filter by selecting a type (Baseline, Evolving, Intermediate,

Advanced, and Innovative). Selected filters show in blue. The statements shown will change with the level selected. To learn more, see the ACET Maturity Results section.

2 Domain header

The domain header contains the component, assessment factors, and statements for the particular domain.

3 Component header

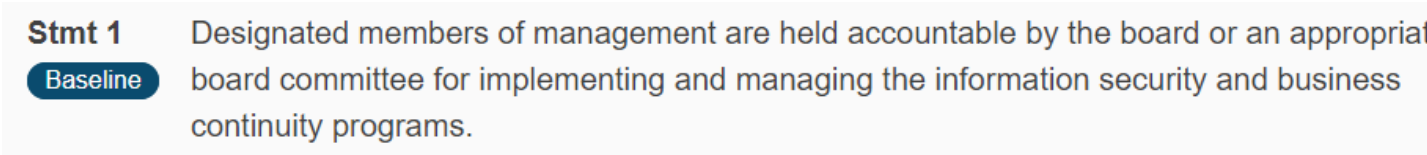


The component header contains the assessment factors and statements for the particular component.

4 Assessment Factor header

The assessment factor contains all statements for the the particular assessment factor.

5 Question/Requirement text



The Statement text contains the exact ACET statements.

Statement Details, Resources, and Comments

The Statement Details, Resources, and Comments contains extra detailed information about the currently selected statement. The user can also add comments, observations, and reference documents to the statement as well as mark the statement for further review. The figure below describes the Statement Details, Resources and Comments screen.

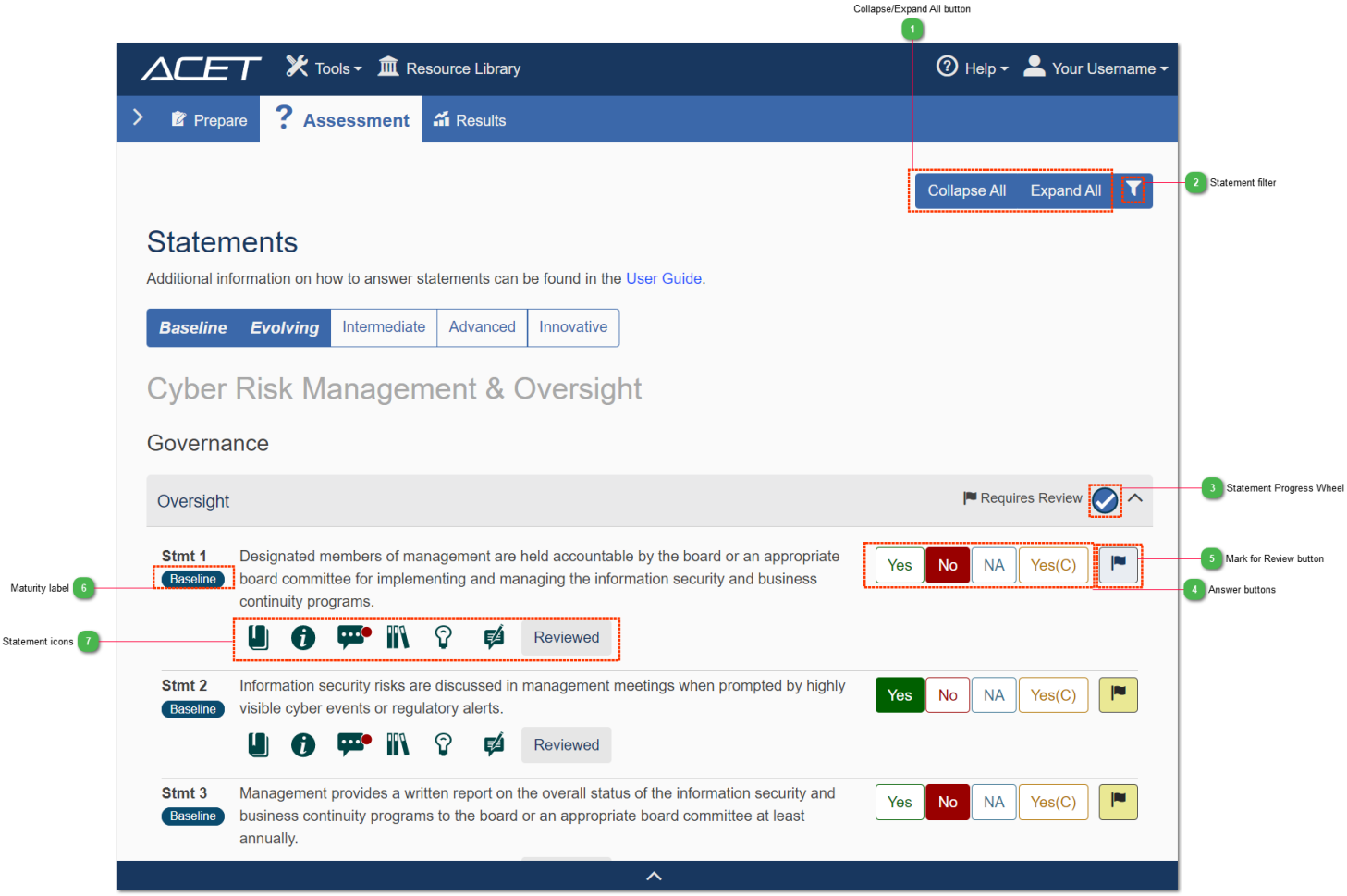


Figure: Statement Details, Resources, and Comments Screen

1 Collapse/Expand All button

Click the Collapse All button to close all question categories, and the Expand All button to open all question categories.

2 Statement filter

Clicking the Statement filter allows the user to filter the assessment statements by answer, whether an assessment has comments, observations, or has been marked for review.

3 Statement Progress Wheel

The Statement Progress Wheel indicates how many questions a user has answered. The checkmark  means that all questions in the category have been answered.

4 Answer buttons

Click "Yes", "No", "NA", or "Yes (C)" to answer questions.

The answers for all questions will be Yes, No, Not Applicable, and Yes (C).
The process is simple. Read the question in detail and then answer yes if the question language and intent are met, or no if the question language and intent are not met.
The colors of the answers reflect the answer given. The colors provide a quick visual reference of how the user is doing in each category.

Yes answers are green, No answers are red, Not Applicable answers are blue, and Yes (C) answers are amber.

In addition to clicking the answers with the mouse, shortcut keys are available to use with this screen. The full list of keyboard shortcuts is available in the help section titled Keyboard Shortcuts.

The Not Applicable is used when the question does not apply to the system or facility.
It should be used with discretion and has the effect of removing the question from consideration.
Any questions marked as Not Applicable will not show up in the online analysis or reports as a gap or missed answer; nor will they count as a positive answer.

The Yes (C) label stands for Yes with Compensating Control. and is used when an alternate or different method is being used
to address the concern in the question. Compensating controls are a consideration when an entity cannot meet a requirement
explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk
associated with the requirement through implementation of other control(s). Comments are required for Yes(C) responses
(to explain the compensating control). A Yes (C) is scored in a positive way similar to a Yes answer.

5 Mark for Review button

The Mark for Review checkbox allows the user to mark a statement for future review.

6 Maturity label

The Maturity label displays the statement's associated Cybersecurity Maturity level.

7 Statement icons

The Statement icons are described in detail below.

Examination Approach button : The Examination Approach button will show or hide detailed examination approaches for each statement.

See the Examination Approach Section for more information.

Supplemental button : Clicking the Supplemental button opens up the supplemental information for the statements.

See the Supplemental Section for more information.

Comments button: Clicking the Comments button opens the Comments Section of the panel allowing the user to enter comments related to the current statement.

See the Comments Section for more information.

References button: Clicking the References button opens the References section of the panel allowing the user to open Standards that are associated with and referenced in the assessment question.

See the References Section for more information.

Observations button: Clicking the Observations button opens the Observations section of the panel allowing the user to create a observation record to associate to the statement.

See the Observations Section for more information.

Reviewed button Reviewed : Users (admins) select the Reviewed button when the statement has been reviewed.

Examination Approach

The Examination Approach section gives additional details into how to examine that the statement is being met.

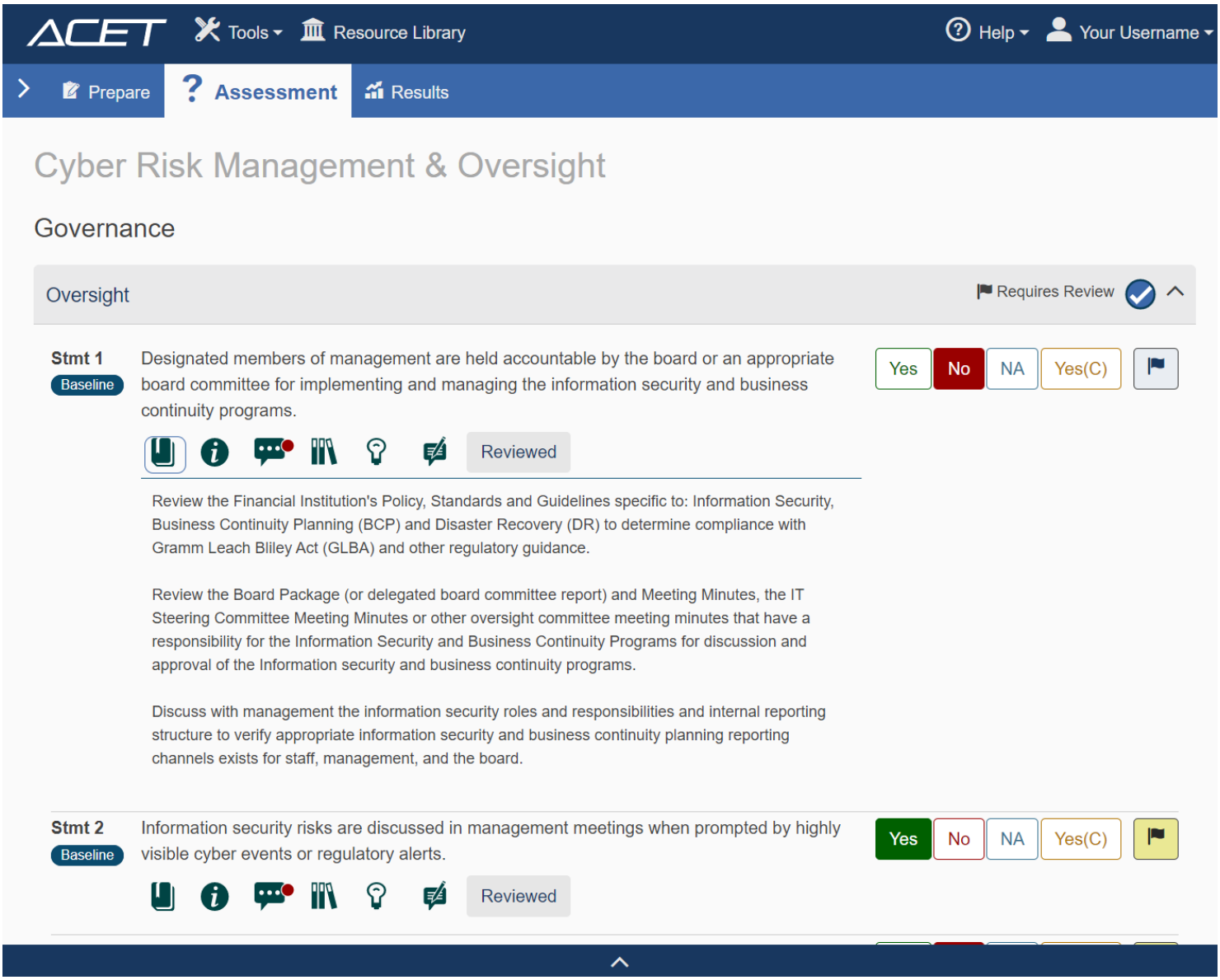


Figure: Examination Approach

Supplemental Section

Staements on the Assessment screen will almost always have supplemental information. The figure below describes the assessment screen focusing on Supplemental information.

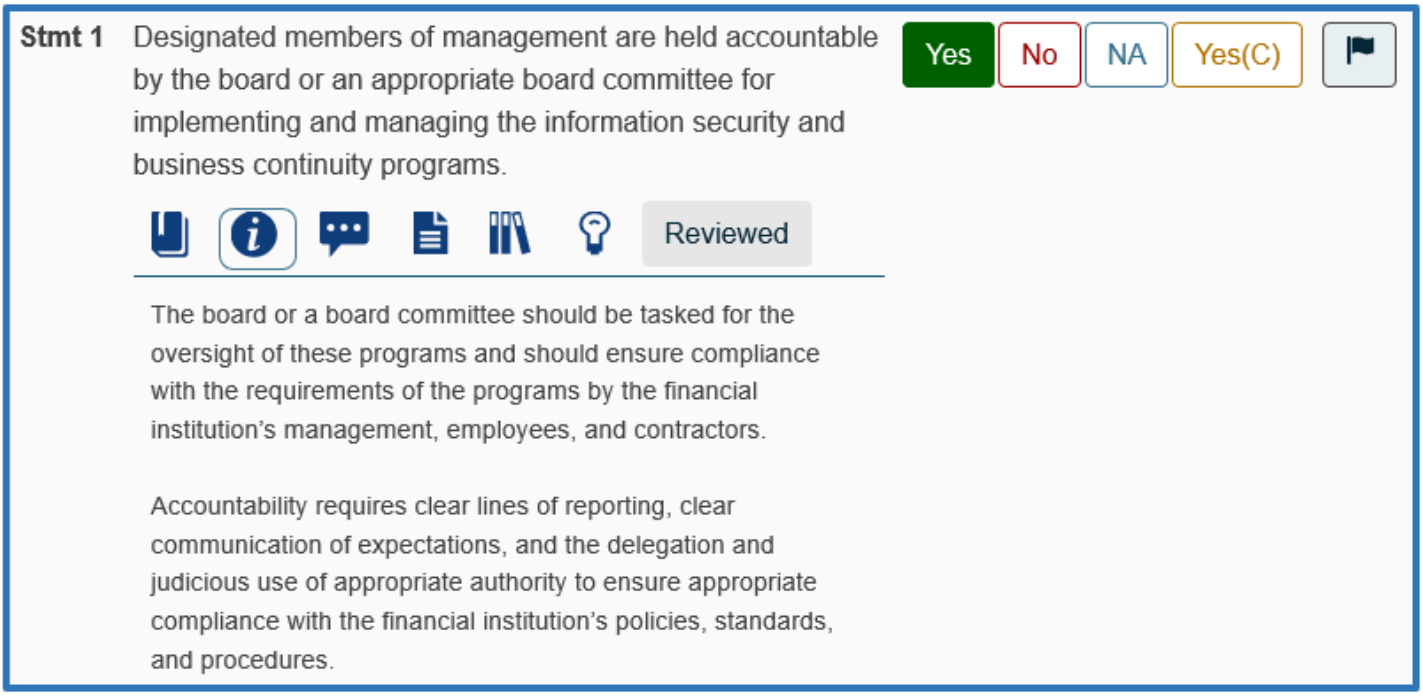


Figure: Question Supplemental Information

Supplemental text: The supplemental text is a readable explanation and elaboration of the subject found in the statement. The text is typically taken from the Standard itself. So statements may exist that do not have supplemental information if they were not included in the Standard. If a set of statements was taken from a single long requirement, the supplemental text may be repeated for multiple questions.

Comments Section

ACET allows the user to add comments to any assessment statement during the assessment process. The figure below describes the comment process.

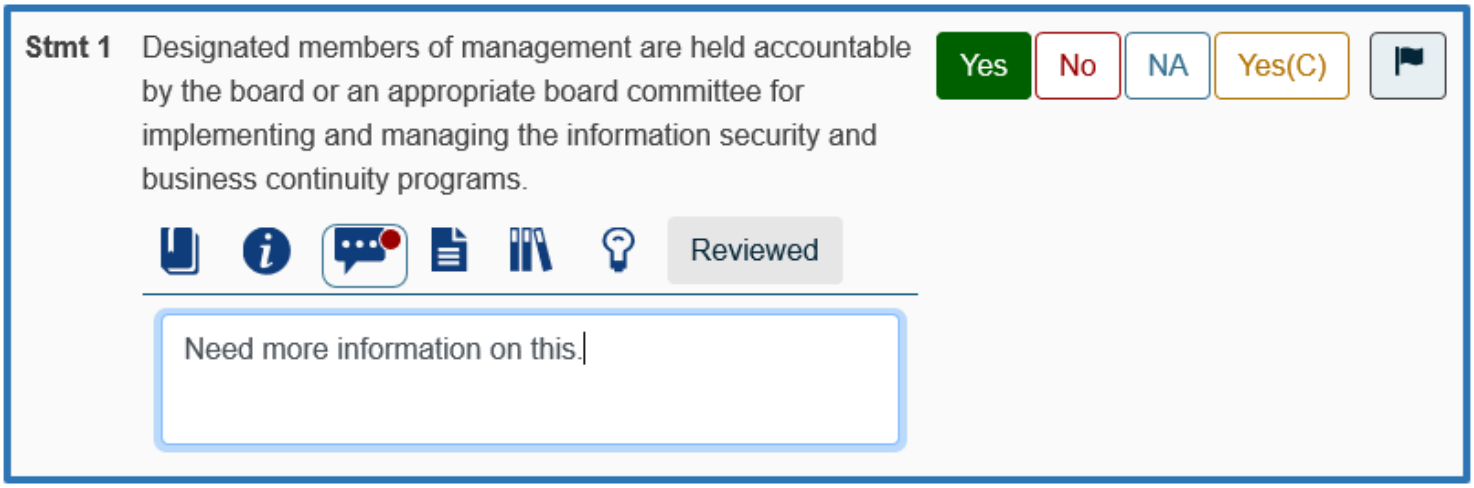


Figure: Assessment Screen Comments Section

Comments field : The Comments button displays a red dot over the comments icon when the statement has comments. This allows the user to easily see what statements have comments when scrolling through the list of questions.

The Comments text box allows the user to add comments or other textual information related to a statement. Comments can be added for multiple reasons such as implementation details, reasons for marking a statement for review, answer justifications, etc.

In some assessments, the Comments input text box is used on rare occasions; in others, the comments are used to record the verification method of answers. This field can be a powerful tool to support the quality of the assessment, especially when documents are also attached to support the answer using empirical data.

References Section

The References Section contains links to related source and Help documentation as seen in the figure below.

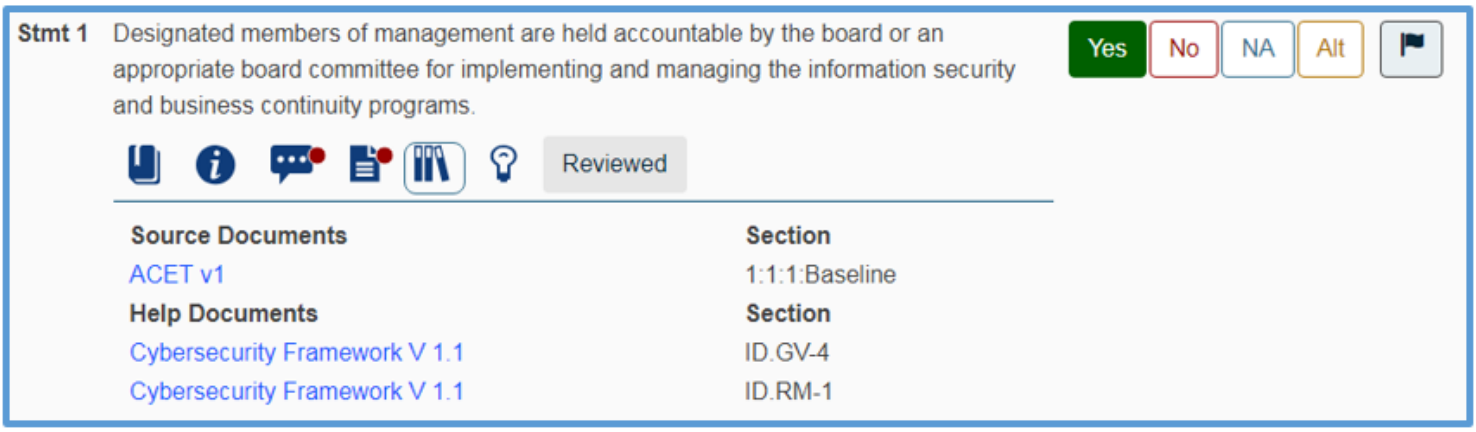


Figure: References Section

References button : The References button displays all references related to the statement.

There will always be at least one source document for the selected Standard. If there is more than one source, then all the sources will be shown in the list of hyperlinks under the title. In most cases, the document will open to the section where the requirement is found.

Observations Section

The Observations Section of the statement details allows the user to associate observations with a statement. The figure below shows the observations section.

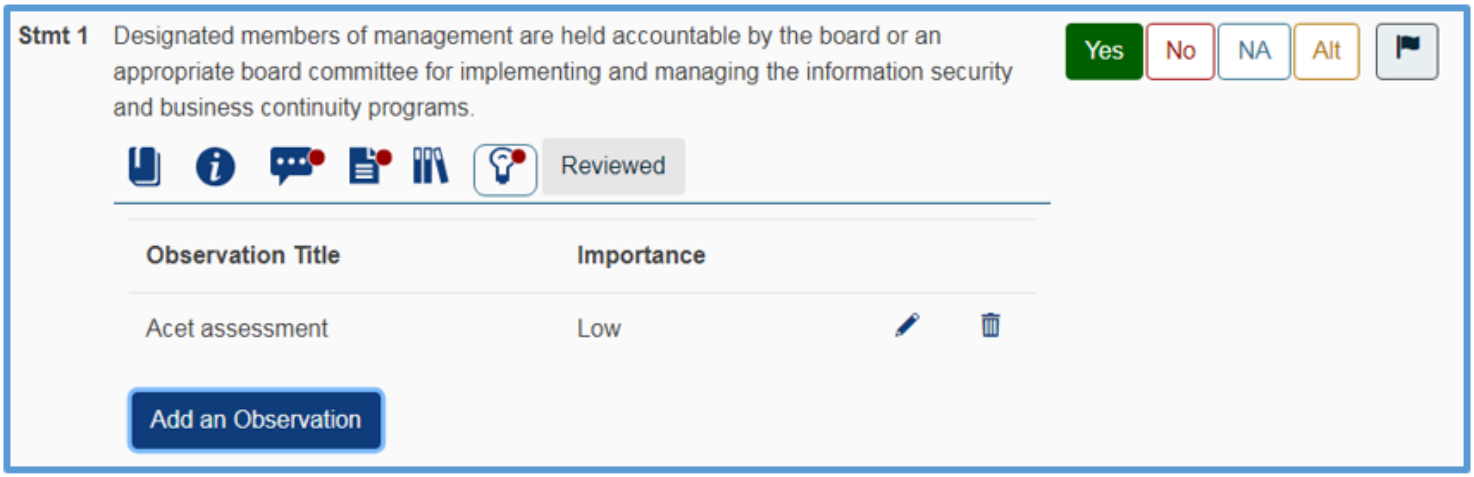


Figure: Observations section

Observations button : The Observation button displays a red dot over the Observation icon when the statement has associated observations. This allows you to easily see what statements have observations when scrolling through the list of questions.

Add an Observation Add an Observation **:** Clicking the Add an Observation button opens the Observations Window that allows the user to enter all statement observation related information.

For more information about the Observations Window, see the Statement Observations help section.

Statement Observations

The observation window allows the user to enter information about a statement that has a "no" answer. Any statement that has been answered "No" could potentially have a observation record. The observation records provide information about the issue, potential impacts of the issue, recommendations for rectifying the issue and potential vulnerabilities related to the issue. Responsible individuals can also be assigned to observation records to be responsible for fixing the problems associated with the observation record. The figure below describes the different parts of the Observation Details window..

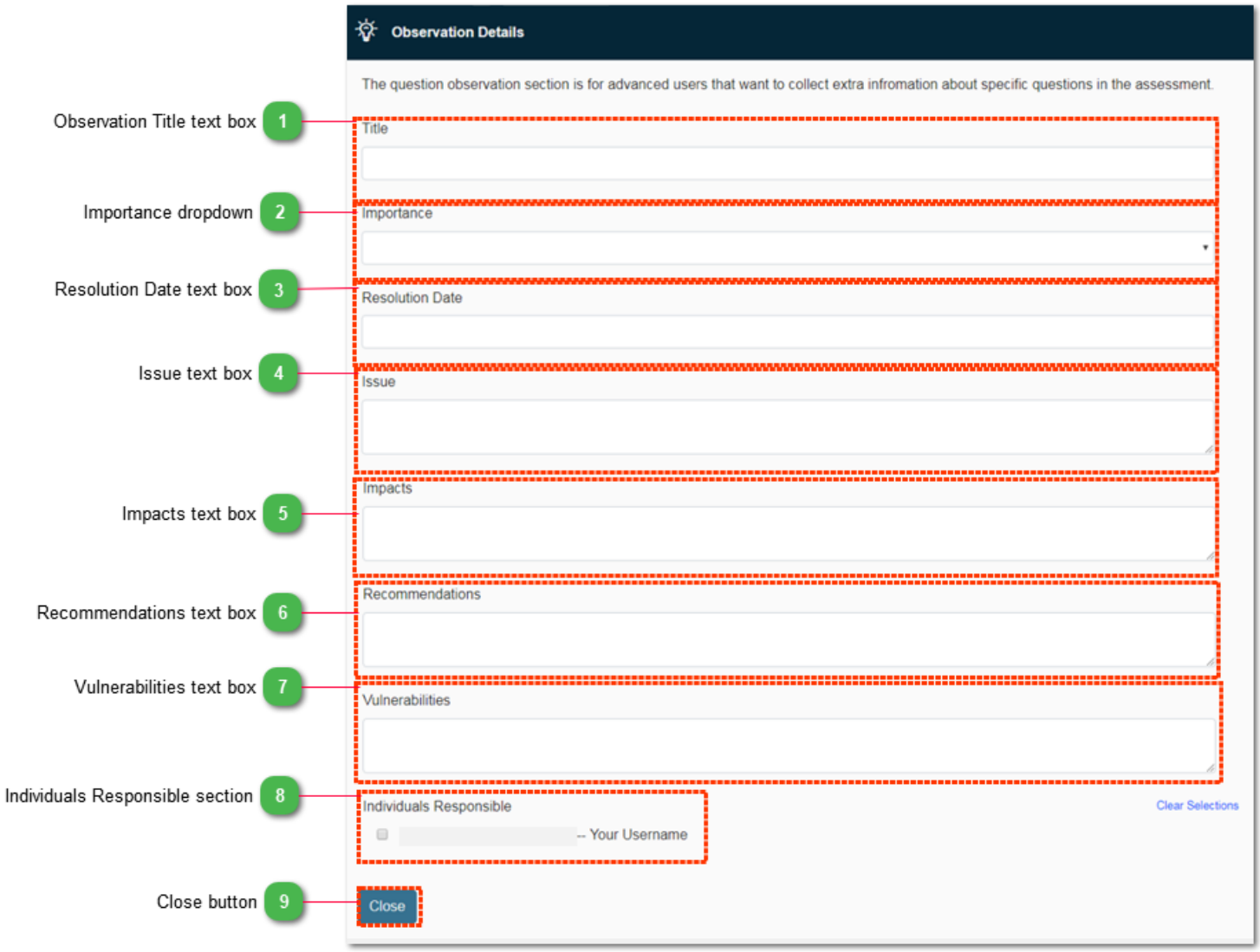
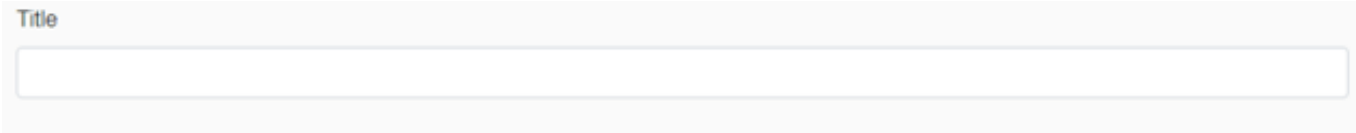


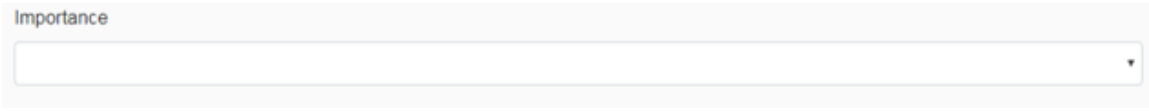
Figure: Observation Details Window

1 Observation Title text box



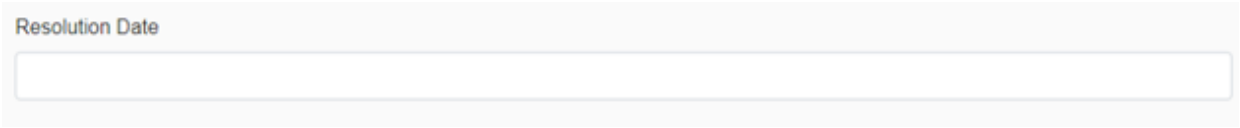
The Observation Title text box corresponds to a Title or Name for the observation record to help the user identify it.

2 Importance dropdown



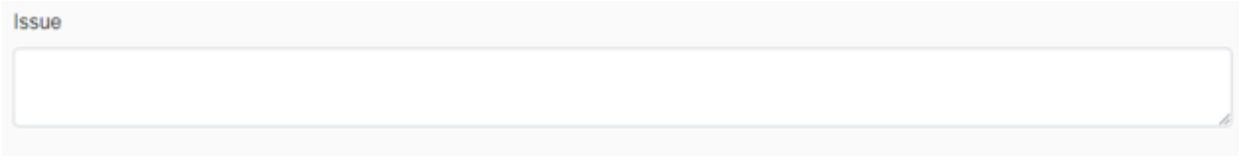
The Importance dropdown allows the user to assign an importance level to the observation record. Valid values are Low, Medium, and High.

3 Resolution Date text box



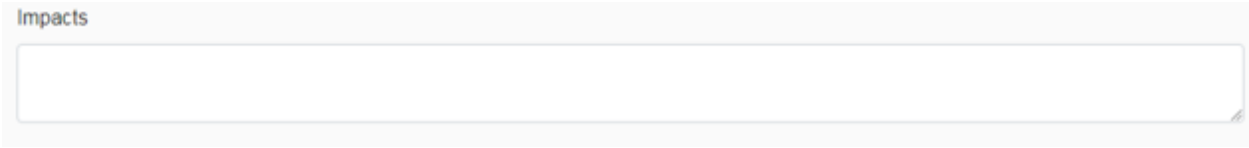
The Resolution Date text box provides input for entering a date when the issue should be resolved.

4 Issue text box



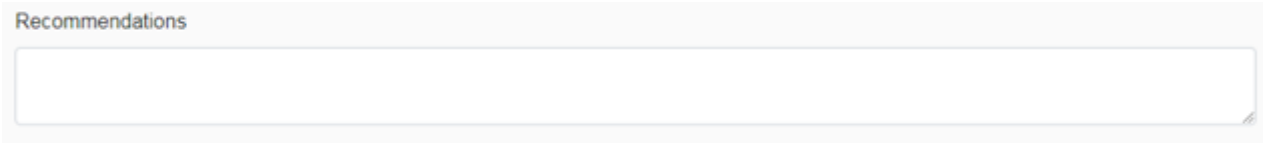
The Issue text box allows the user to define a detailed explanation of the issue or problem related to why the statement was answered "No".

5 Impacts text box



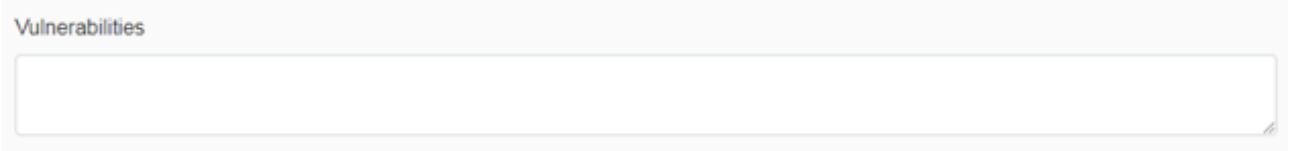
The Impacts text box allows the user to define potential or real impacts that the issue may or is currently having on systems, assets, and/or procedures.

6 Recommendations text box



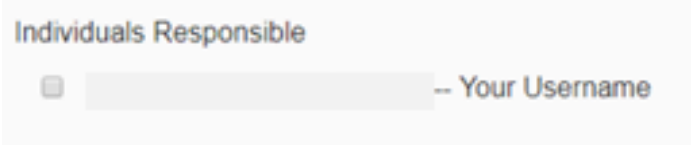
The Recommendations text box allows the user to provide recommendations or steps for resolving the issues or problems defined in the observation.

7 Vulnerabilities text box



The Vulnerabilities text box allows the user to identify any known vulnerabilities on systems or assets related to the observation.

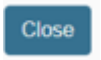
8 Individuals Responsible section



NOTE: This section isn't available in ACET only mode.

The Individuals Responsible section allows the user to assign individuals to be responsible for fixing the issues identified in the observation record. The Contacts check list will contain a list of all current contacts associated with the assessment. Selecting a contact will associate an individual to be responsible for the observation record.

9 Close button



The Close button will close the Observations Details window.

Statements Filter

Use the Statements Filter to limit the Statement types you see. The user can filter on answer type (Yes, No, NA, Yes(C), Unanswered) or added observations, comments, and marked for review.

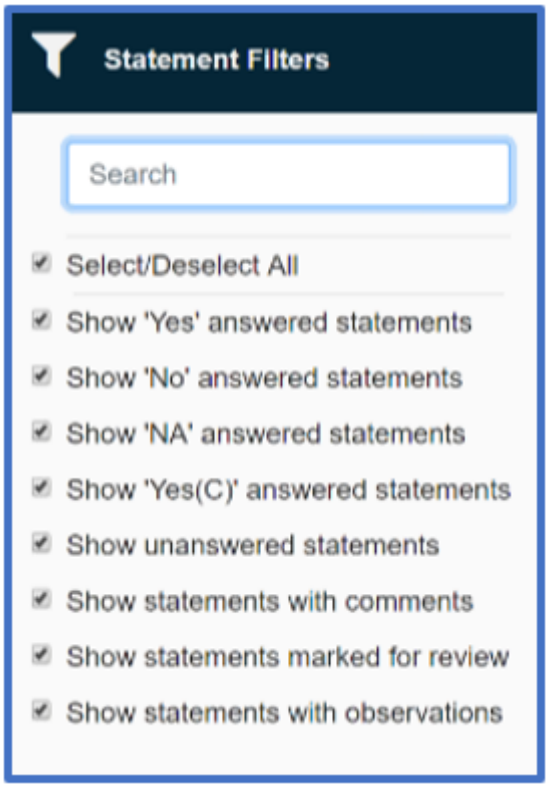


Figure: Statement Filter

You can select as many filters as they would like to combine, select all, or select none.

A message will appear if there are no results to show so that you can change your selection.

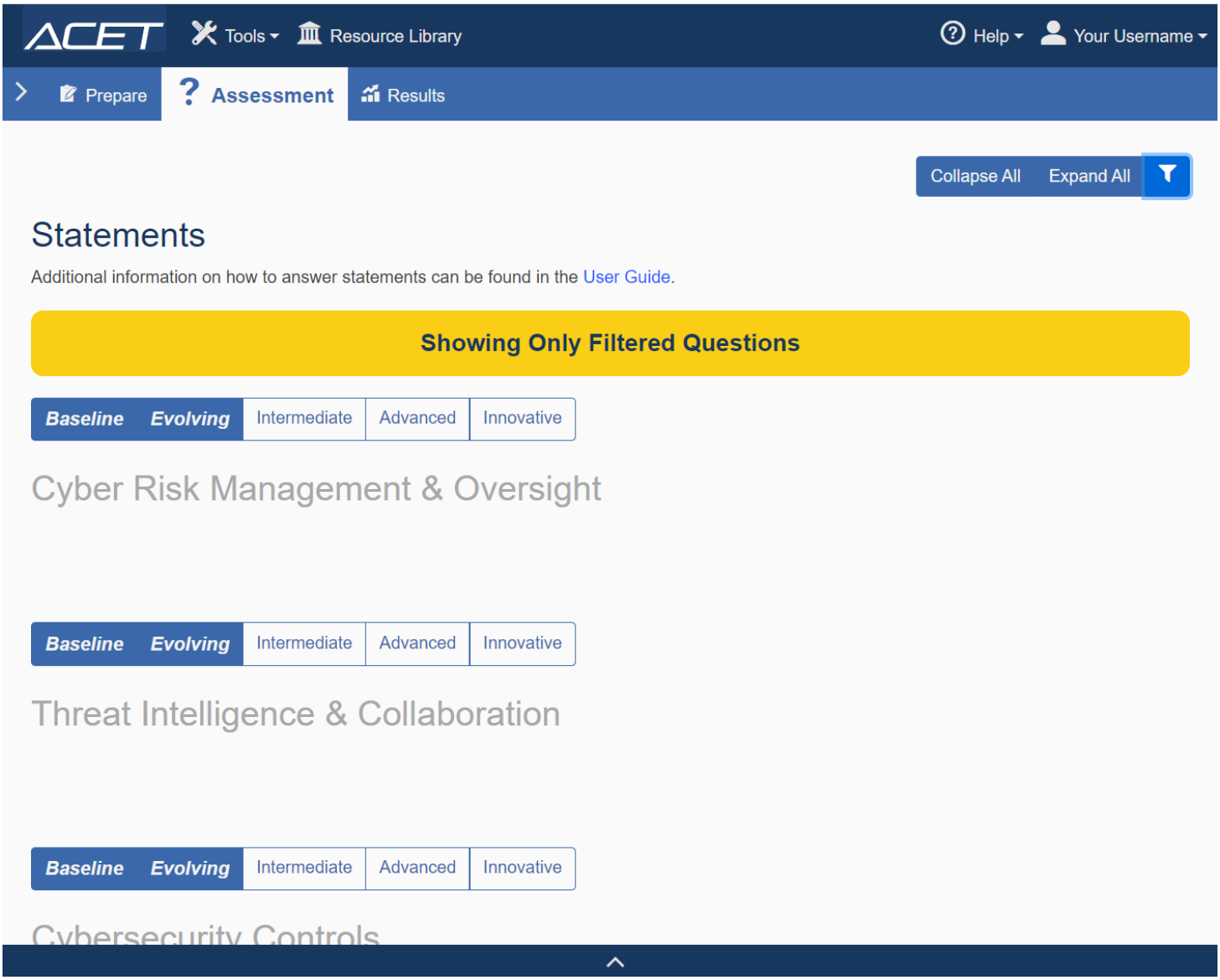


Figure: No results visible error message

Results Section

Once Standards and SAL have been selected and the resulting statements have been answered, it is time to analyze the results of the assessment. Two methods are available to review and analyze the results. The first uses the online Results screens and the second approach is to print the reports and review the hardcopy.

The Results section provides a method to measure security posture based on the selected Standards and the statements answered during the assessment process. The Results section uses charts and tabular data to provide a visual display of the data and at the same time allows for comparisons across categories, statements, and subject areas.

The Results sections consists of the Analysis Dashboard and charts, and the Reports. This section will describe each area.

Analysis Screen

The Analysis screen provides a quick visual view of how well the user is doing related to the user's cybersecurity posture. The Analysis screen consists of the Analysis Navigation Section, the Chart Section, and Results Navigation Section.

The figure below describes the sections of the Analysis screen.

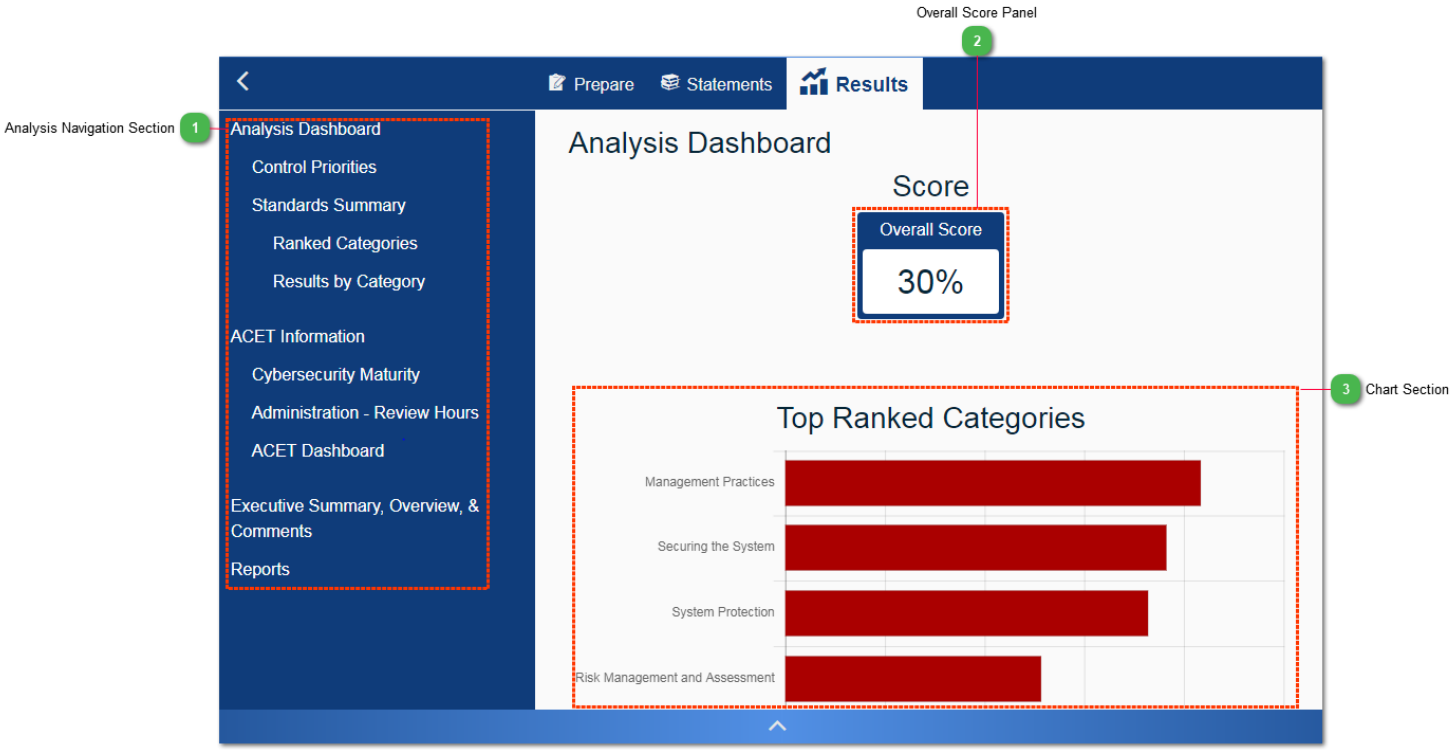
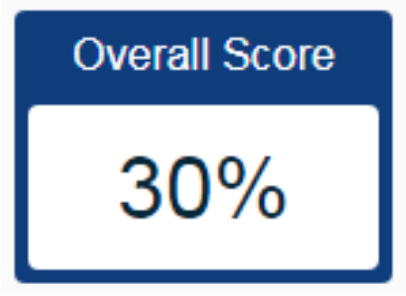


Figure: Analysis Screen

1 Analysis Navigation Section

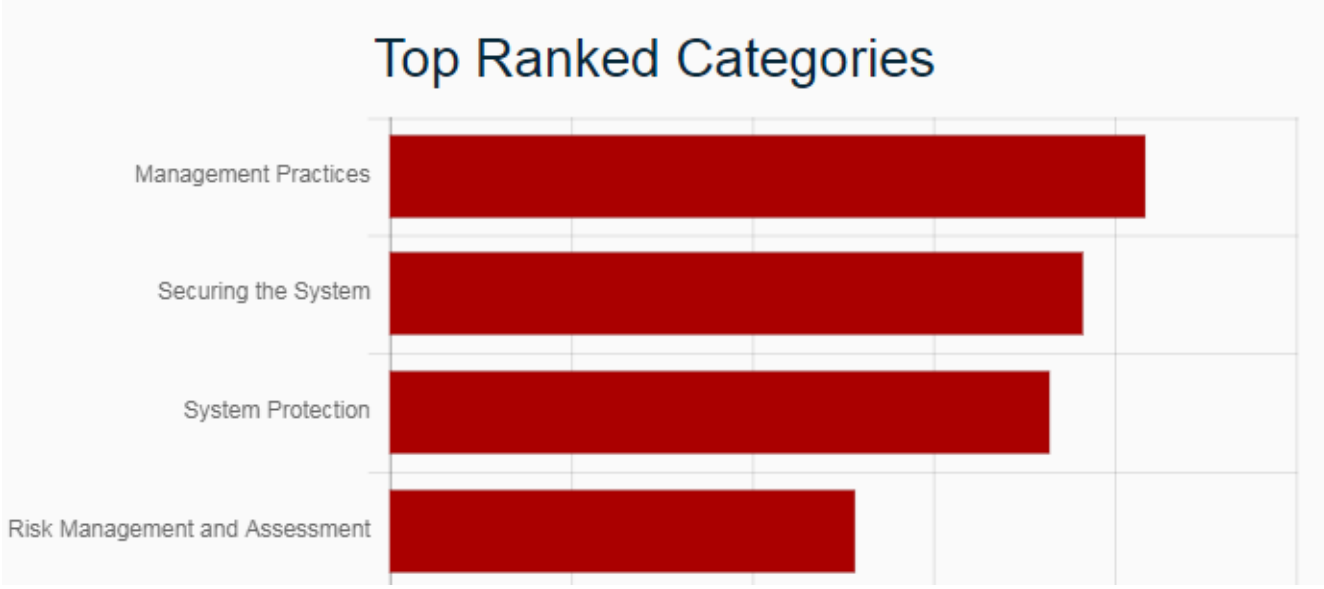
The Analysis Navigation section contains links for accessing the different navigation screens. Most links are divided into categories where the details can be hidden or displayed to facilitate working with the many options available.

2 Overall Score Panel



The Overall score is calculated based on how many statements were answered "Yes" or "Yes(C)" versus the total number of statements.

3 Chart Section



The Chart section is where the charts and tabular data are displayed. Generally, the user can place the mouse cursor over a chart section to see the value associated with the section of the chart. Tabular data are also available to view or export on most screens.

Analysis Dashboard

The Analysis Dashboard shows the Top Ranked Categories and Standards Summary for quick reference. The figure below provides a brief description of the Analysis Dashboard.

Top Ranked Categories:

The Top Ranked Categories chart provides a quick look at the top six categories where the user needs to improve the most or the highest priority categories on which to focus attention first based on the assessment answers.

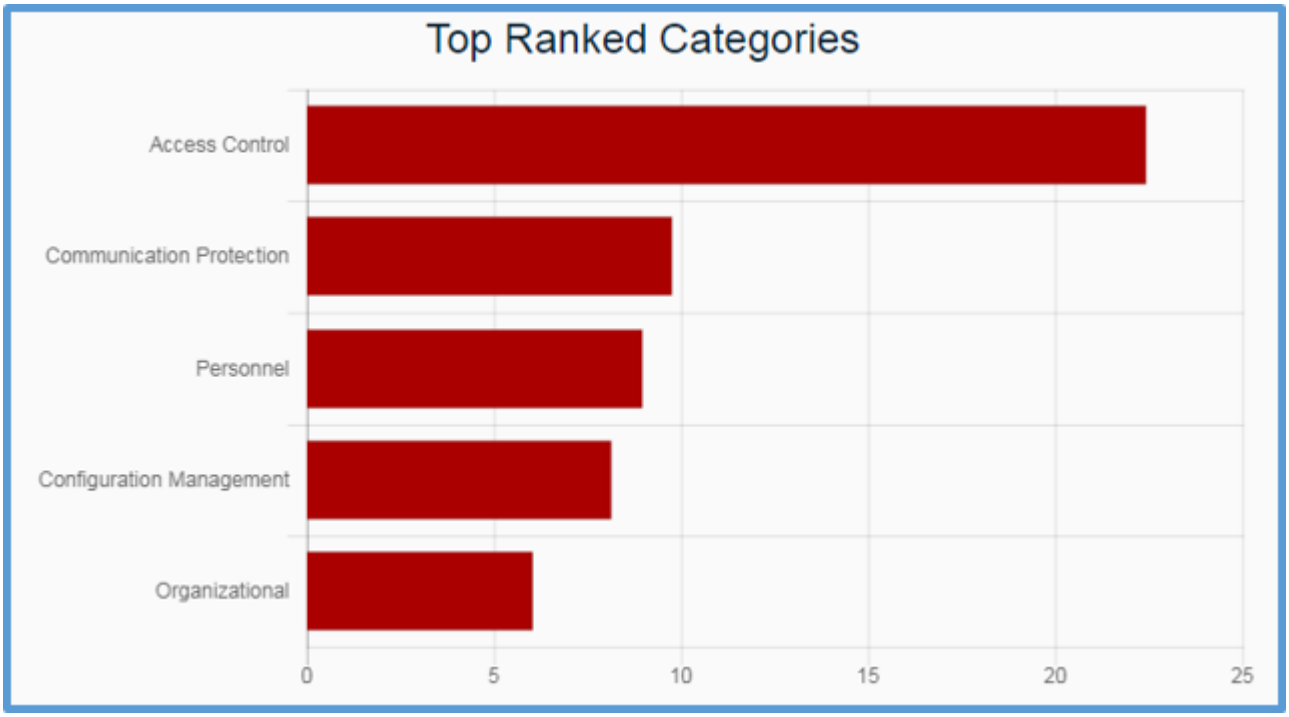


Figure: Top Ranked Categories chart

Standards Summary:

The Standards Summary chart provides a quick look at the percentages of how the user answered the Standards-based questions.

For more information about the Standards Summary chart and data, see the Standards Summary help section.

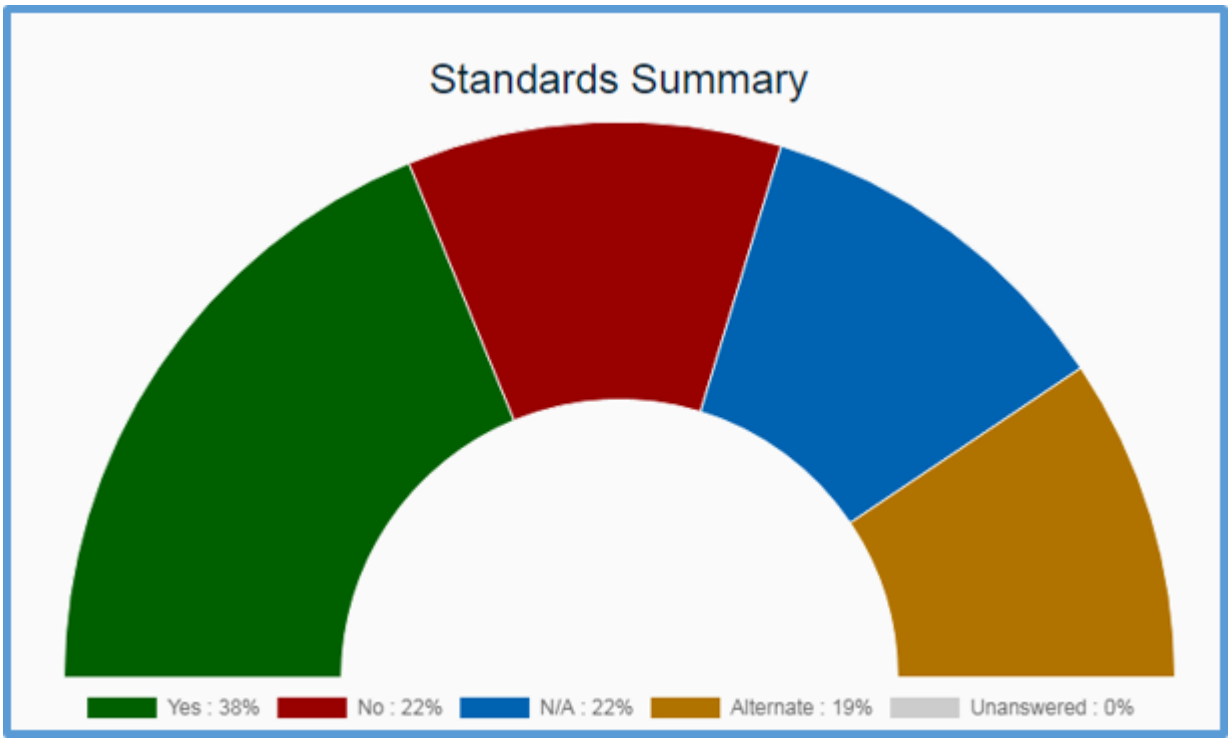


Figure: Standards Summary chart

Control Priorities

Each statement in the assessment where the answer had a No response or was unanswered will be ranked and displayed on the Control Priorities Screen. The information provided is intended to answer the fundamental question, "Okay, I have some problems, so what do I do first?" Based on the ranking, the answer would be, do Number 1 first, and then do Number 2, and so on until all resources have been exhausted or all the problems have been resolved.

The Control Priorities screen is shown in the figure below.

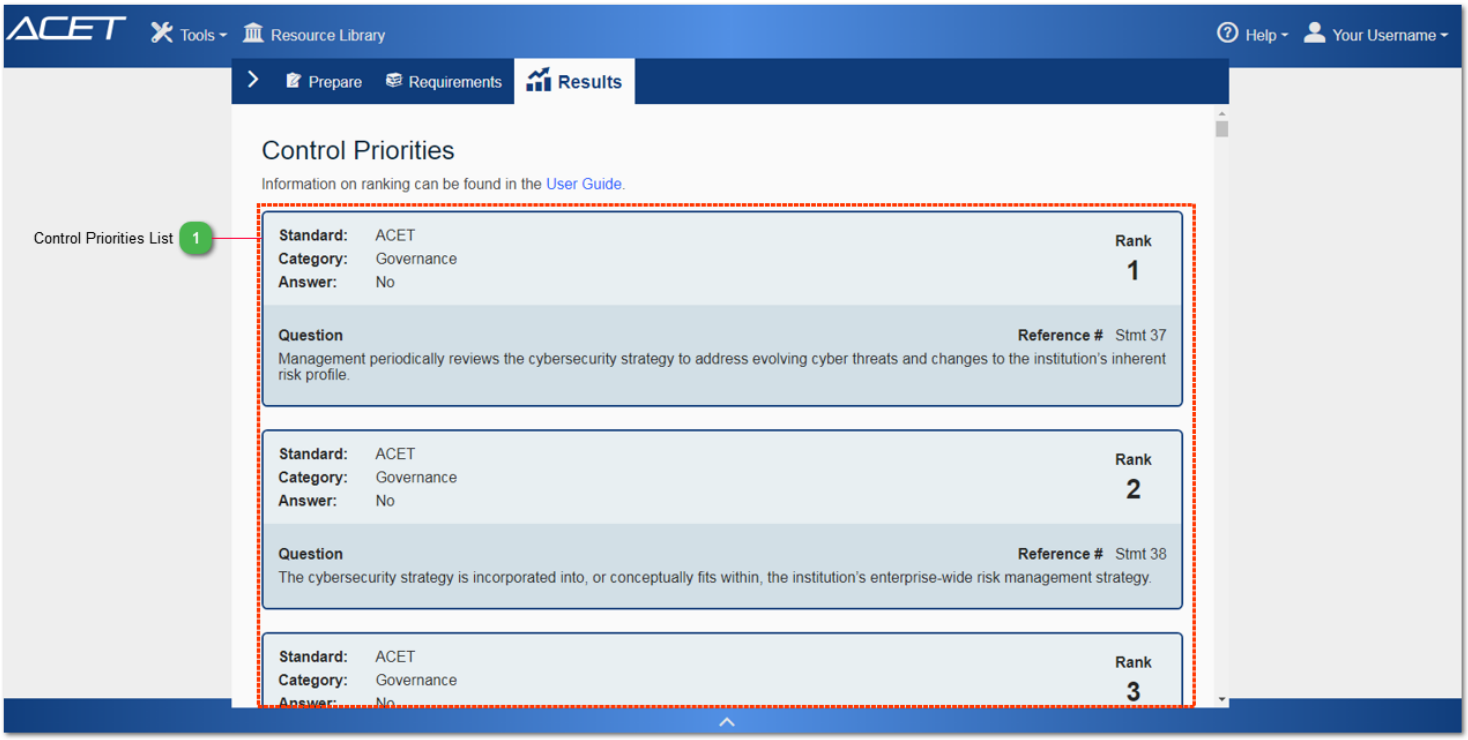
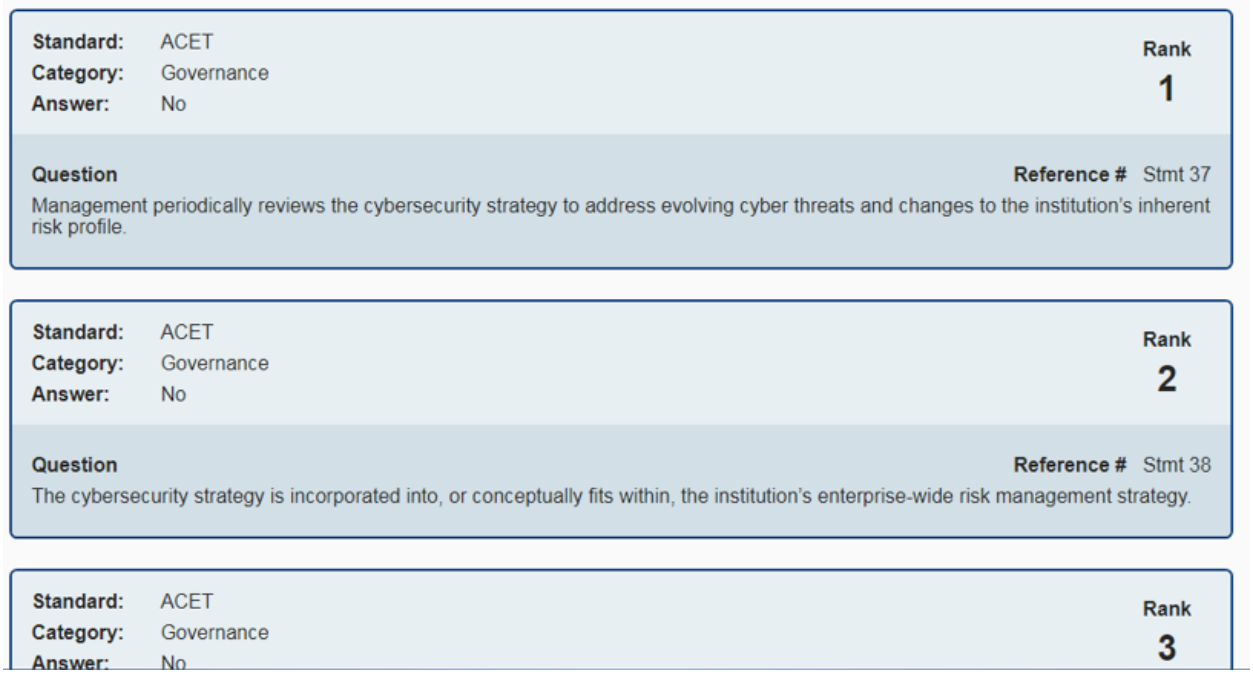


Figure: Control Priorities Screen

1 Control Priorities List



The Control Priorities list displays a list of all statements that were answered 'No' or left unanswered.

The following is a description of the columns in the Control Priorities List:

Rank:

A numeric ranking of each statement that was missed with #1 having the highest priority.

The ranking is based on a combination of factors that all impact the overall score.
The factors include the following:

The specific weighting value assigned to each statement in ACET.

This weighting comes from subject matter experts with years of experience in information technology and control system cybersecurity. The statements were analyzed and assigned a weight relative to all other statements.

The weighting value of the subject area or statement category.

Each area was also given a weight by experts relative to all other areas.
Like the statement itself, it was determined that some areas are more important than others, even though they are all important to cybersecurity.

The security assurance level (SAL) of the question (when using a standard other than ACET).

Each question is linked to an assurance level. For example, a question that is associated with a Very High level
would be lower in rank than one with a Low level, because it is recommended that the user work on the basic
requirements before moving to those required for a higher level. A good example relates to access control.
Users should implement a complex password, (or maybe even a password) before worrying about
implementing system access controlled by a combination of a complex password, physical token, and biometrics.
The SAL will only affect the weighting when the score is higher than a Low for the facility.
Because the SAL limits the questions to only those matching the SAL value,
if the score is at a Low, then the user would never see any questions that might
be marked as Moderate, High, or Very High.

Standard Name:

The value in this column identifies the Standard from which the statement came.
This concept is especially important when using multiple Standards that have the same category names.
The combination of Standard Name, Category, and # will help locate the exact statement.

Category:

The title of the main question category or subject area where the statement is found.

Number or #:

This column identifies the statement number in the Standard and category.

Question:

The text from the statement.

Answer:

This is the answer selected when completing the assessment.

The data can be sorted by clicking its corresponding column header
but it is recommended to keep the statements in Ranked order and address them accordingly.

Standards Analysis

The Standards Analysis section of the Analysis Navigation panel displays charts and tabular data based on answers to statements for the selected Standards. Standards Analysis contains analysis screens for Summary, Ranked Categories, and Results by Category that will be described in the following sections.

Standards Summary

The Standards Summary Single Standard screen shows summary information related to the results from the answers to the single Standard that was selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only.

The data displayed corresponds to answers to statements associated with only the selected Standard.

The chart shows the percentage of all Yes, No, NA, Yes(C), and Unanswered statements for the selected Standard. The tabular data show the Answer in the first column. The second column indicates the number of the indicated answer, the third column shows the overall total number of statements, and the final column shows the percentage of the number for the total.

The Standards Summary Single Standard screen is shown in the figure below.

Figure: Standards Summary Single Standard Screen

Ranked Categories

The Ranked Categories screen shows a list of all main categories ranked in order of the categories that should be prioritized based on how the statements were answered. Only answers from the selected Standards are included on this screen. Diagram component answers are not included. The chart shows the categories ranked in order of importance.

This screen highlights the categories that need the most attention for failed Standards based questions. Unlike other analysis screens that highlight the positive answers, this screen and the associated data show what categories or areas are weakest and what needs the most attention. In other words, the longer the bar in the chart, the worse the score in that area.

The Data Tab contains the tabular data of the categories that match the bars on the associated chart. There are five columns in the tabular data:

Category:
The categories are taken from the list of categories associated with the selected Standards. If multiple Standards are selected then this list is made up of the universal categories. Questions from a single Standard use the categories from that Standard.

Rank:
The Rank column corresponds to the size of the bar on the chart and is an importance weighting.

For more information about how categories are ranked, see the Category Rankings help section.

Failed:
The Failed count shows the number of negative answers determined by either a No or Unanswered answer. The total number of statements does not include statements marked as not applicable.

Total:
The Total indicates the total number of statements within the indicated category.

Percent:
This column is the number of failed answers divided by the total number of statements to get the percentage.

The Ranked Categories screen is shown in the figure below.

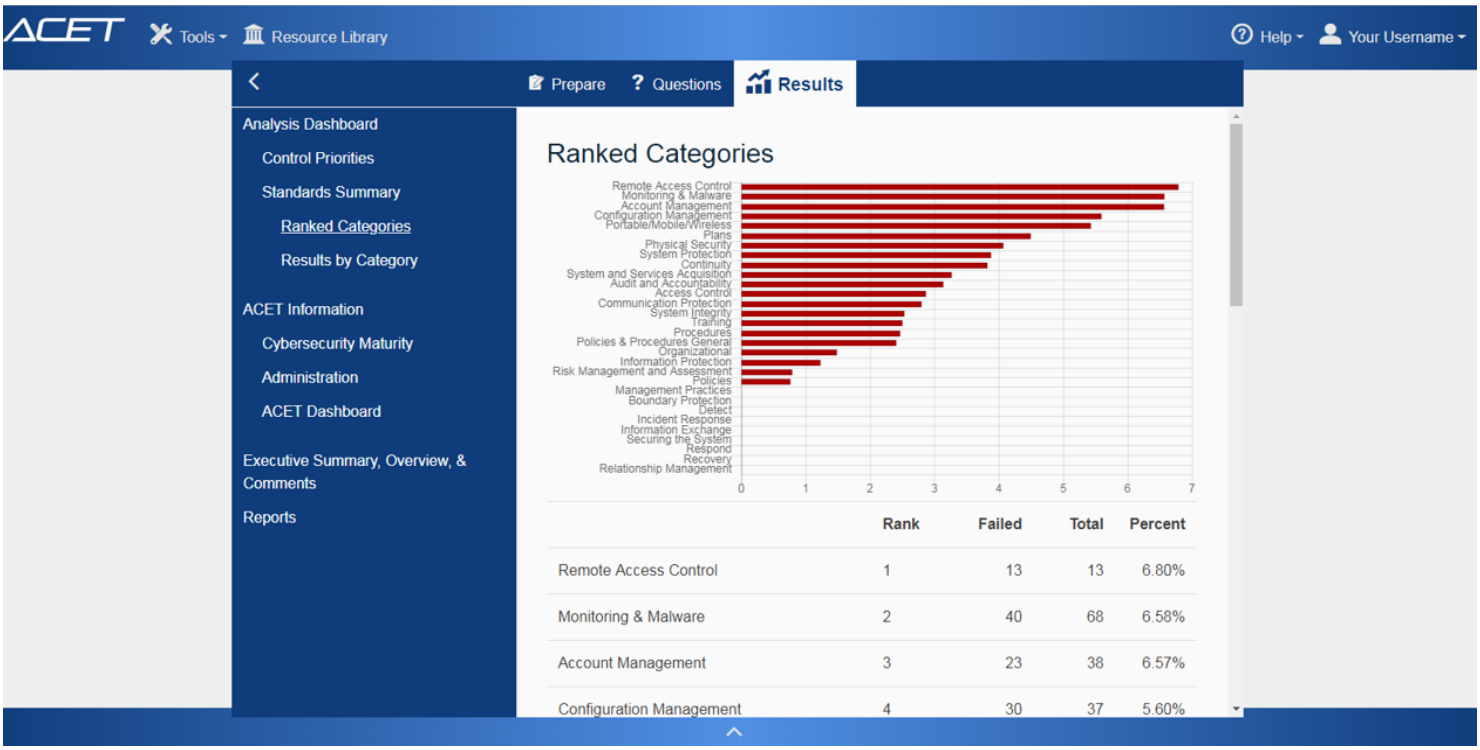


Figure: Ranked Categories Screen

Results by Category Single Standard

The Results by Category Single Standard screen shows the positive results of how the user performed on the assessment organized by the category in which the statements are grouped. The results are based on statements from a single Standard selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only. If multiple Standards are selected, the Results By Category Multiple Standards screen is displayed..

The chart displayed is a bar chart and shows the percentage of passed (Yes and Alternate or Yes(C)) answers to statements for the selected Standard grouped into categories. The Data Tab shows the Category in the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of statements in the category, and the final column shows the percentage of the passed answers over the total.

The Results by Category Single Standard screen is shown in the figure below.

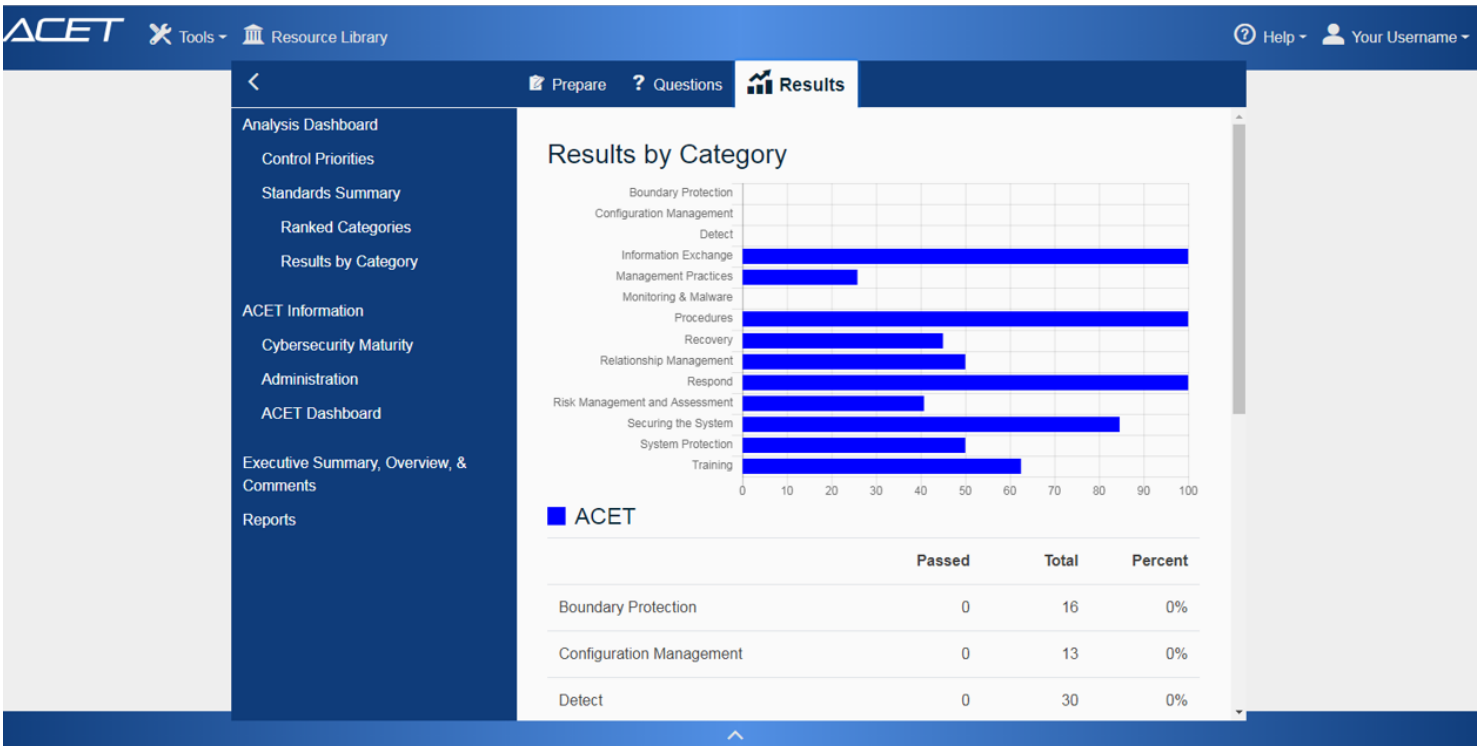


Figure: Results by Category Single Standard Screen

Results by Category Multiple Standards

The Results by Category Multiple Standards screen shows the positive results of how the user performed on the assessment organized by the selected Standards as well as the category in which the questions are grouped. The results are based on questions from multiple Standards selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to multiple Standards. If a single Standard is selected, the Results By Category Single Standard screen will be displayed. The data displayed also do not include data related to components on the network diagram.

The chart displayed is a multiple bar chart. For each category, the chart displays a bar for each selected Standard. Each bar shows the percentage of passed (Yes and Alternate or Yes(C)) answers to questions for the indicated Standard. The Data Tab shows multiple tables, one for each Standard, with the Category as the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of questions in the category, and the final column shows the percentage of the passed answers over the total.

The main ACET window may need to be maximized in order to read the chart appropriately.

The Results by Category Multiple Standards screen is shown in the figure below.

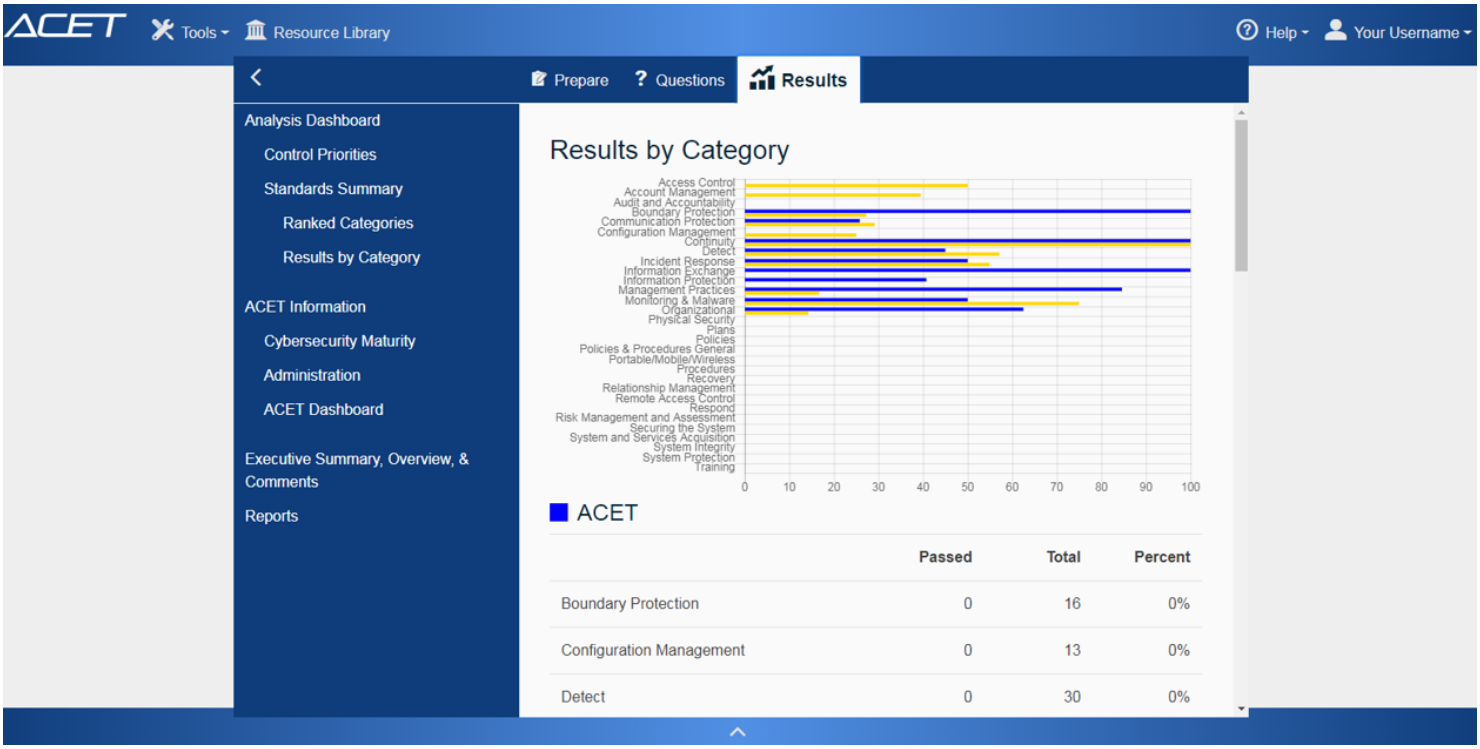


Figure: Results by Category Multiple Standards Screen

Category Rankings

Each Standard has an overall defined risk. This overall risk is determined from the number of questions and the weight of each question. The weights of questions have been determined by cyber security experts. If all questions have been completely failed then the ranked category bar charts will show that the user is at 100% of the risk defined by the Standard as seen in Figure: Ranked Categories with 0%. If about half the questions were answered yes, then the graph would only show the user at 50% of the overall risk as seen in Figure: Ranked Categories with 50%. See the two graphs below.

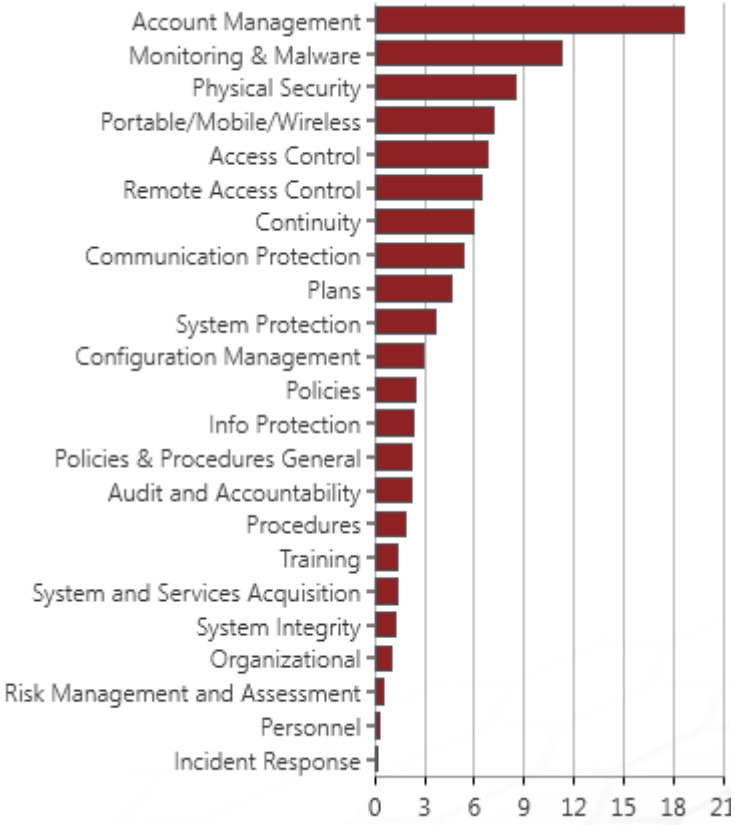


Figure: Ranked Categories with 0% of Account Management Questions Passed

Figure: Ranked Categories with 50% of Account Management Questions Passed

Note that the x-axis is different between Figures Ranked Categories with 0% and Ranked Categories with 50%. Otherwise the graphs look about the same. The x-axis changes because the proportions of risk are the same. According to this Standard, the Monitoring and Malware controls consume about 2/3 of the risk that Account Management does. However, if we go back and answer a great majority of Account Management questions as Yes then we obtain the chart in Figure: Ranked Categories with 100%.

Figure 138. Ranked Categories with 100% of Account Management Questions Passed

Now the risk accounted for from the Account Management section is only about 1% of the original risk defined by this Standard. Note that Monitoring and Malware still Accounts for about 6% of the overall risk as it did above.

ACET Information

The ACET Information section of the Results tab includes Cybersecurity Maturity, Administration, and ACET Dashboard.

To learn more select an option below.

ACET Maturity Results

The Maturity Detail worksheet summarizes the results for each Domain. The Domain statements are answered within the Statements tab. To learn more about the statement answering process, see the Assessment Section.

Within each domain are assessment factors and contributing components. Under each component, there are declarative statements describing an activity that supports the assessment factor at that level of maturity.

Each maturity level includes a set of declarative statements that describe how the behaviors, practices and processes of an institution consistently produce the desired outcomes. The Assessment starts at the Baseline maturity level and progresses to the highest maturity, the Innovative level. An item marked as Incomplete has not been completely answered. An item that has been fully answered but does not meet the Baseline level is designated AdHoc.

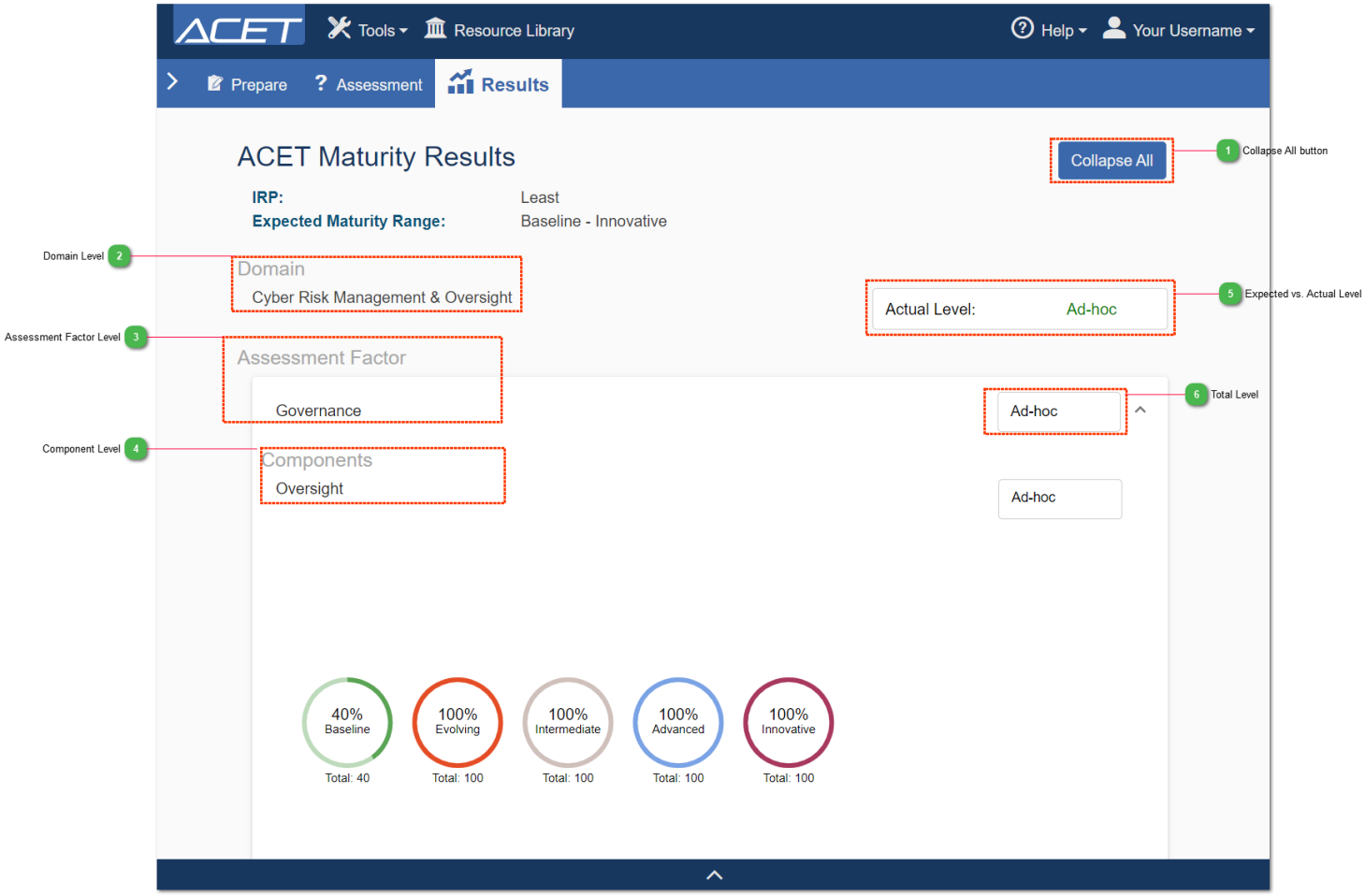
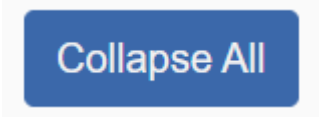


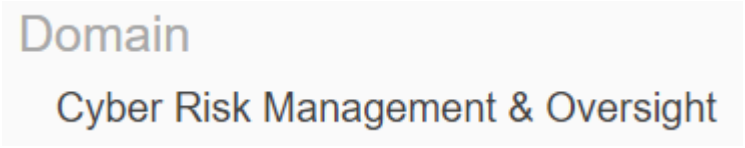
Figure: Cybersecurity Maturity screen

1 Collapse All button



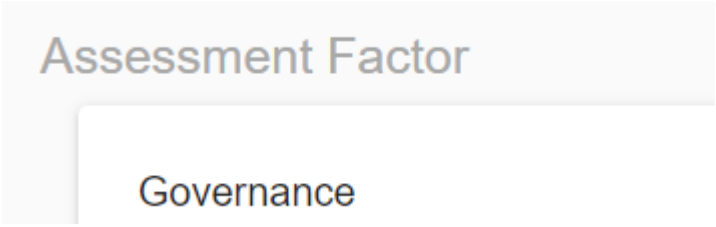
Select the Collapse All button to close to the assessment factor level. The screen defaults to expanded. Click Expand All to return to the default.

2 Domain Level



The domain level shows the combined risk level of all the assessment factors and components within the domain. If anything within the domain is incomplete the top-level (domain level) will remain incomplete.

3 Assessment Factor Level



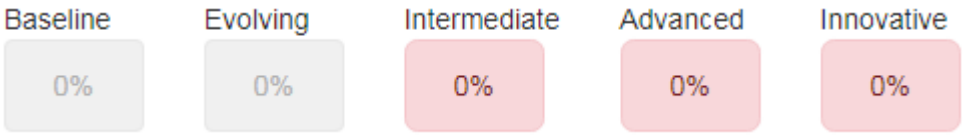
The assessment factor level displays the roll-up for each components within it.

4 Component Level

The component levels show what percent compliant a user is based on their answers per domain. The final level is shown in blue and is rolled up to Assessment Factor and then, finally, to Domain.

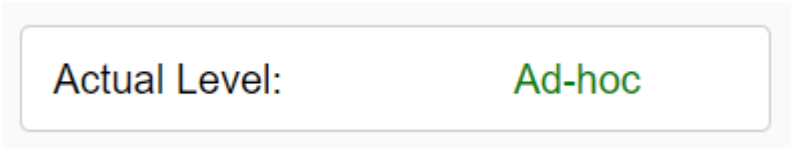
The colors for the components level is defined below:

Gray= Isn't necessary for user to answer based on their assigned level
Red= 0% for assigned level
Yellow= 1-99% "No" answers do not count toward the percentage
Green= 100% all statements answered



Component levels that user's do not need to answer are shown in gray. The levels that need to be answered, but haven't been completed are shown in red.

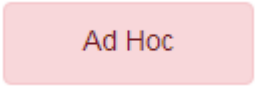
5 Expected vs. Actual Level



The expected vs. actual levels show the user's expected level based on IRP and Maturity. The actual level shows what the user has answered in the Statements tab.

6 Total Level

Each component and assessment factor has a total level. If it is gray and says "Incomplete" the statements have not been answered.



If it is red and says "Ad Hoc" then the statements have been fully answered but does not meet the Baseline level.

Total levels go from Incomplete to Ad Hoc, Baseline, Evolving, Intermediate, Advanced, and Innovative.

ACET Dashboard

The Dashboard's primary functions are to summarize the information input from the Assessment, Inherent Risk Profile, and Administration screens.

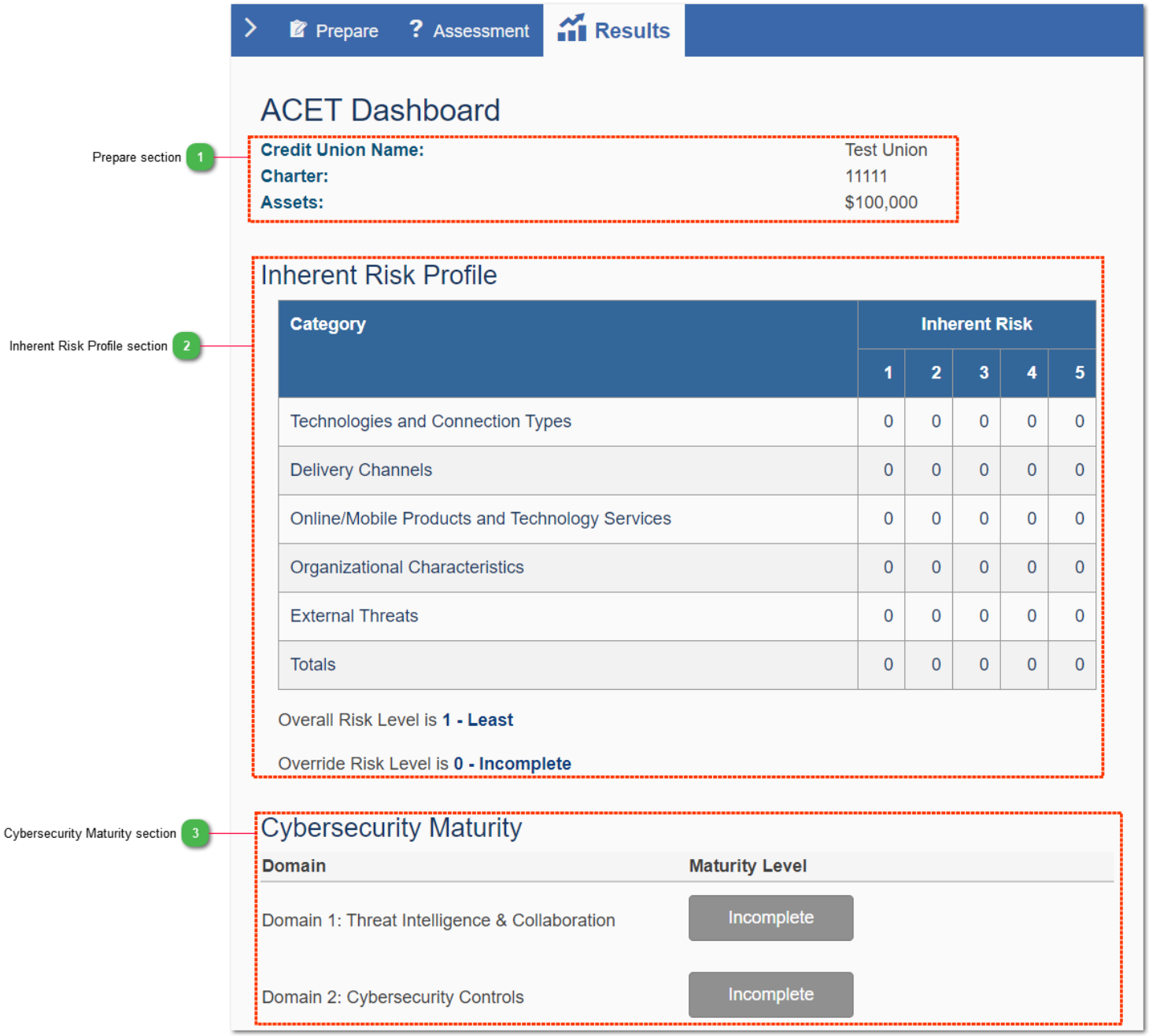


Figure: ACET Dashboard

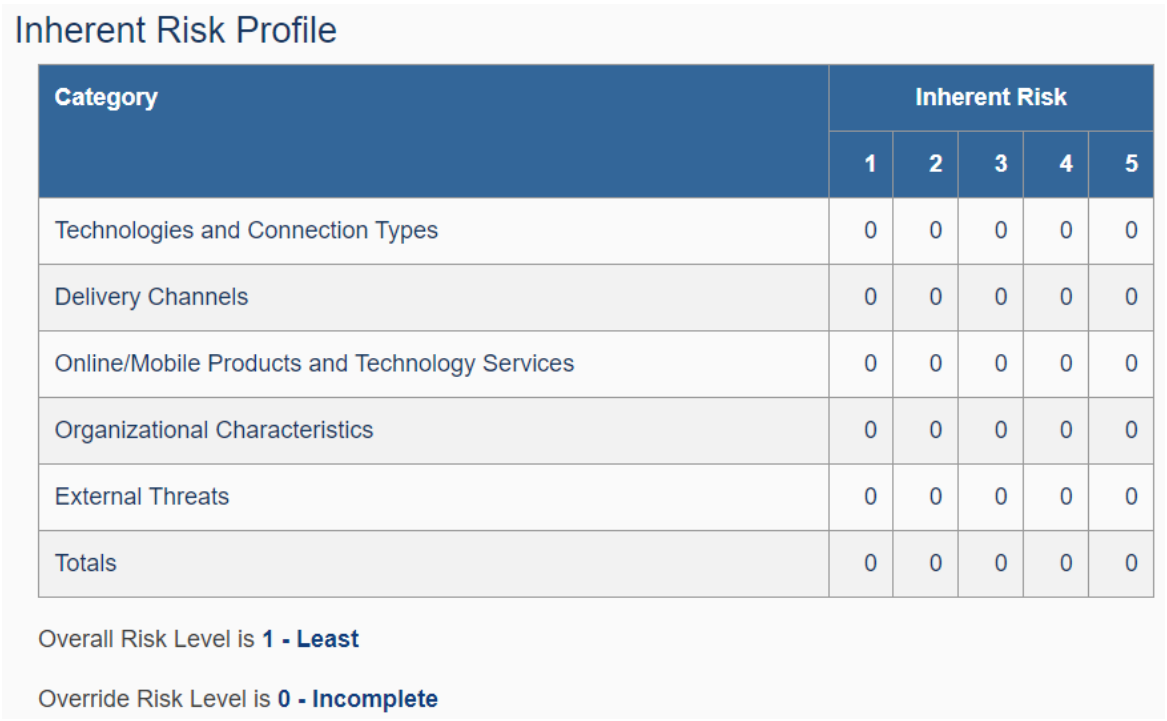
The Dashboard provides the credit union demographic information. It also summarizes information from other worksheets in the workbook. There are three sections to the Dashboard:

1 Prepare section

Credit Union Name:	Test Union
Charter:	11111
Assets:	$100,000

Exam Preparation section contains demographic information from the Assessment Details section, and the Total Hours from the Administration screen.

2 Inherent Risk Profile section



Inherent Risk Profile

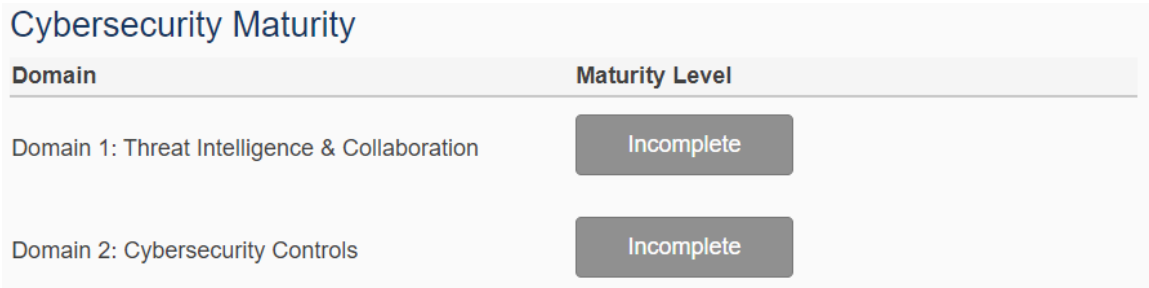
Category	Inherent Risk				
	1	2	3	4	5
Technologies and Connection Types	0	0	0	0	0
Delivery Channels	0	0	0	0	0
Online/Mobile Products and Technology Services	0	0	0	0	0
Organizational Characteristics	0	0	0	0	0
External Threats	0	0	0	0	0
Totals	0	0	0	0	0

Overall Risk Level is **1 - Least**

Override Risk Level is **0 - Incomplete**

The Inherent Risk Profile (IRP) section repeats information found in the Inherent Risk Summary screen.

3 Cybersecurity Maturity section



Cybersecurity Maturity

Domain	Maturity Level
Domain 1: Threat Intelligence & Collaboration	Incomplete
Domain 2: Cybersecurity Controls	Incomplete

The Cybersecurity Maturity section summarizes the maturity levels. The maturity levels will show as “Incomplete” until responses for all of the statements in the Baseline maturity for each Domain are complete.

Reports Section

After the assessment is complete users can generate reports.

The intent of the reporting function is to provide a way to print and publish assessment information, including summary charts and lists. It also provides a hardcopy of the results to be used in meetings, for communications to management, and as a way to assign tasks to technical staff. Combined with the online analysis, these reports can help the user clearly understand where weaknesses are and where improvements should be made.

This section will describe how to use the Reports Screen.

Executive Summary, Overview, and Comments Screen

The Executive Summary, Overview, and Comments screen allows the user to add executive level information for display on the Executive Summary report. As well as, a high-level description of the assessment and any relevant comments to be displayed on the reports.

Some default text is provided on the Executive Summary screen; however, the user should replace that text with actual summary information that captures the highlights of the assessment as seen in the figure below.

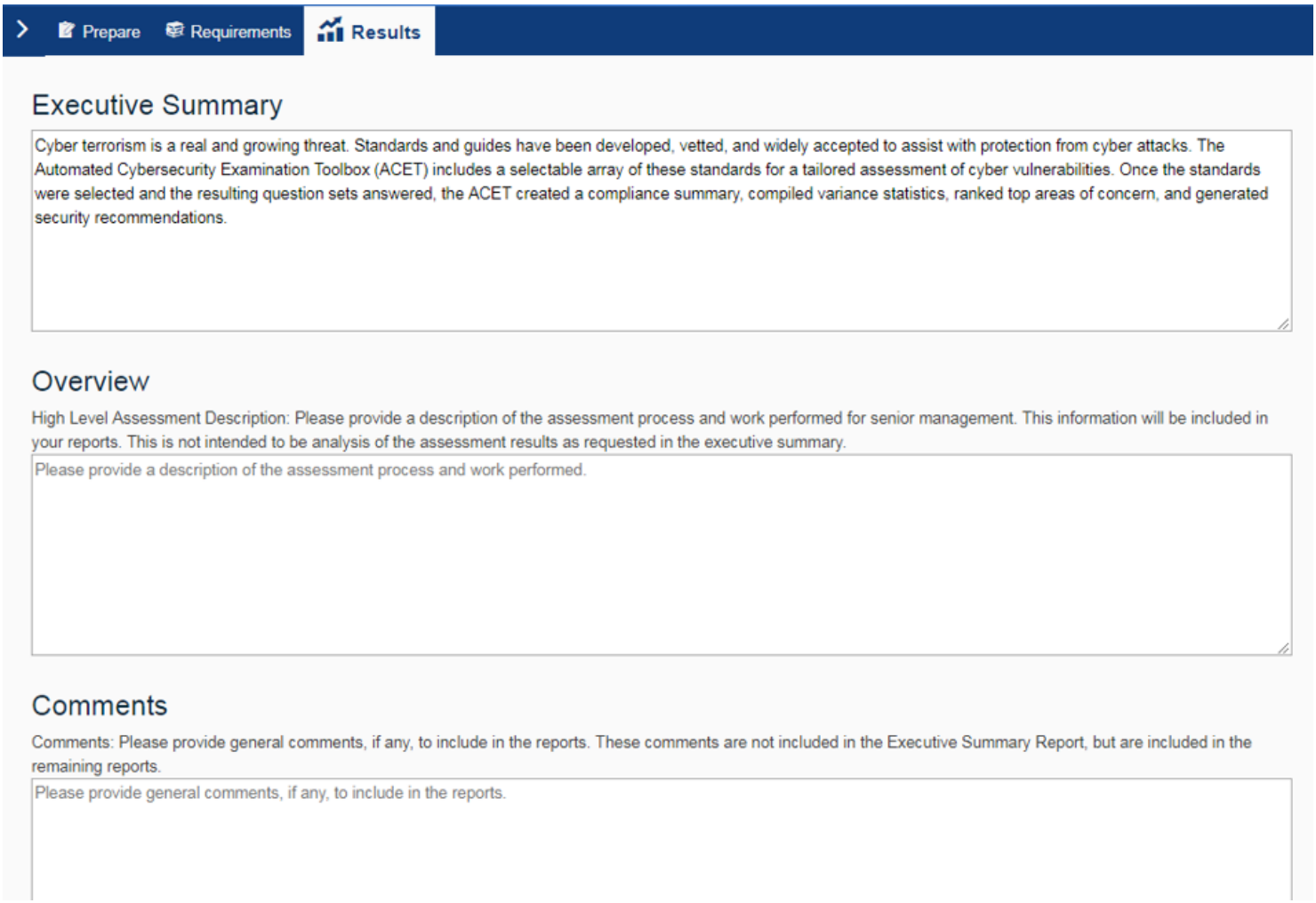


Figure: Executive Summary Screen

Report Builder

The Report Builder screen is shown in the figure below.

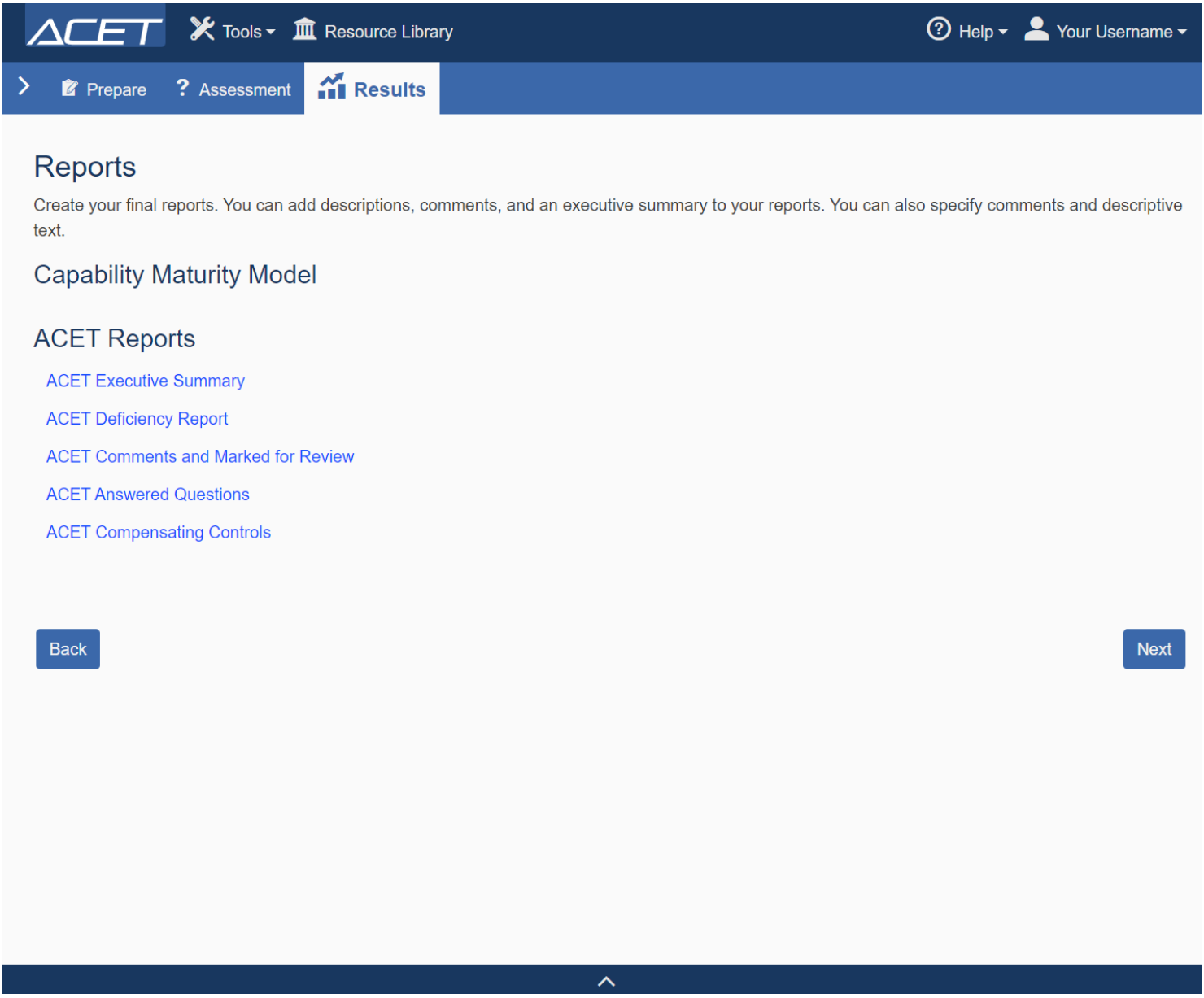


Figure: Report Builder screen

To generate a report click on the specific report link on the Report Builder screen. The report will open in a new tab.

To learn more about the individual reports, see Executive Summary, Deficiency, Comments and Marked for Review, Answered Statements, and Compensating Controls.

Executive Summary

The Executive Summary Report is designed for an executive level audience. The intent is to provide limited graphical and high level, summary information that can be understood quickly.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, the name of the person that was entered in the Principal Assessor/Name field, and the Asset value entered in the Assessment Configuration screen.

Site Information: Site Information includes all of the information entered on the Assessment Configuration screen.

Maturity Detail: Maturity Detail is an output of the Cybersecurity Maturity screen. It summarizes the results for each Domain based on your answers within the Assessment tab.

Inherent Risk Profile: This screen is an output of the Inherent Risk Profile Summary screen. It summarizes what you selected in the Inherent Risk Profile screen.

Cybersecurity Maturity: This screen is an output of the Cybersecurity graphic on the ACET dashboard. It gives a high-level view of your maturity levels per domain.

Deficiency

This deficiency report lists the statements that are not currently compliant or "No" answers.

This is often referred to as the GAP Report. This report intends to list the gaps, assist users of the report in identifying gaps, prioritizing work, and beginning to make a plan to address the gaps by implementing the controls necessary to come into compliance with the associated statement.

The percentage gap in each domain is also listed and will help to determine the priority. ACET is a cumulative maturity model meaning lower levels should be completed before moving to higher levels. Ideally baseline should be completed before focusing efforts on controls in evolving and so forth up the line of maturity levels.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, the name of the person that was entered in the Principal Assessor/Name field, and the Asset value entered in the Assessment Configuration screen.

Deficiencies: The Deficiencies table shows each statement that was answered "No", any comments associated with the statement, and whether or not it was marked for review.

Comments and Marked for Review

This report includes all statements that were marked for review and any statements with an associated comment.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, the name of the person that was entered in the Principal Assessor/Name field, and the Asset value entered in the Assessment Configuration screen.

Questions Marked for Review: The Marked for Review table shows statement text and any comments associated with the statements marked for review.

Statement Comments: The Comments table shows the statement text and comment for all statements with comments, as well as, if they have been marked for review.

Answered Statements

This report includes all the statements within your maturity level, your answers, and whether there is a comment attached to the statement.

The statement set is determined by your maturity level.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, the name of the person that was entered in the Principal Assessor/Name field, and the Asset value entered in the Assessment Configuration screen.

Answered Statements: The Answered Statements table displays all answered statements, what they were answered (Yes, No, N/A, or Yes(c), the maturity level, and whether there is a comment associated.

Compensating Controls

This report contains all the statements that have an associated compensating control and the comment provided.

Title Page: Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, the name of the person that was entered in the Principal Assessor/Name field, and the Asset value entered in the Assessment Configuration screen.

Compensating Controls: The Compensating Controls table shows each statement that was answered "Yes(c)", their associated compensating comments, and any additional comments associated with the statement, and whether or not it was marked for review.

Glossary

Acronyms

Acronym	Definition
ACET	Automated Cybersecurity Evaluation Toolbox
ALT	Alternate Method
C2M2	Cybersecurity Capability Maturity Model
CAG	Consensus Audit Guidelines
CCI	Control Correlation Identifier
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CMMS	• Computerized Maintenance Management System
CNSSI	Committee on National Security Systems Instruction
CoR	Catalog of Recommendations
ACET	Automated Cybersecurity Examination Tool
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DHS	U. S. Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	U. S. Department of Defense
DRL	Document Request List
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act of 1996
HMI	Human-Machine Interface
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IIS	Internet Information Services
INGAA	Interstate Natural Gas Association of America
IR	Interagency Report
IRP	Inherent Risk Profile
IT	Information Technology
MAC	Mission Assurance Category
MIL	Maturity Indicator Level
MSC	Multiple Services Component
NA	Not Applicable
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
PCIDSS	Payment Card Industry Data Security Standard

PDF	Portable Document Format
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
RBPS	Risk-Based Performance Standards
RG	Regulatory Guidelines
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition
SP800	Special Publication 800
TSA	Transportation Security Administration
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

Key Terms

Term	Explanation
Admin Questions	Questions spawned by the tool in response to the applied Standards the user selects.
Assessment Documents	Repository of documents added to the assessment by the user.
Assessment Report	A summary report of results for each question including user responses, statement of actual requirements (or deficiencies), answers in relation to the overall SAL, and associated help documents.
Classified Information	Any information or material that has been determined by the U.S. Government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security (Classified Information Procedures Act, 18 U.S. Code App. 3, Section 1(a)).
Component Diagram or Network Diagram	A network topology that best represents the industrial control system configuration. Diagram includes typical components associated with a control system such as connector, firewall, network router, network switch, serial switch, network hub, modem, programmable logic controller, remote terminal unit, HMI, engineering workstation, intrusion detection system, wireless access point, serial radio, application server, database server, terminal server, web server, virtual private network, link encryption, DCS, printer, and clock.
Component Questions	A generated list of control system cybersecurity questions based on the defined SAL and components contained within the network topology diagram.
Confidentiality Level	Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoD has three defined confidentiality levels: classified, sensitive, and public.
Critical Asset	Those facilities, systems, and equipment, which if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories: MAC I, MAC II, and MAC III. MAC I systems require the most stringent protection measures.
Public Information	Official information that has been reviewed and approved for public release by the information owner.
Resource Library	Electronic copies of cybersecurity documentation are included in the tool for reference, including federal codes, white papers, reports, industry Standards, and guidelines.
Security Assurance Level	The relative consequences of a successful attack against the control system being evaluated. The consequence analysis identifies the worst, reasonable consequence that could be generated by a specific threat scenario. The General SAL provides an overall rating of the criticality based on the users' review of security threat scenarios and estimated consequences. The SAL ranges from Low to Very High.
Security Categories	The security categories are related to the NIST 800-53 Standards and are defined as: CONFIDENTIALITY "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information. INTEGRITY "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information. AVAILABILITY "Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system.
Security Categorization	The NIST 800-53-related security categorizations of Low, Moderate, and High are explained as: LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii)

	result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Security Level	The rating of High, Moderate, or Low for Confidentiality, Integrity, and Availability according to FIPS 199 and NIST SP800-60.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.

Frequently Asked Questions (FAQs)

This is a list of questions that new users may find helpful.

My system is running slow. How can I make it go faster?

This release may run slower than previous releases of ACET. Check to make sure that there is sufficient RAM on the user's computer. 3 GB of RAM is recommended. Check the Task Manager to verify that the computer is not paging to the disk drive, which would cause a significant drop in performance. The delays typically come from the system loading and caching data between the main screens. There is a greater delay when using a large diagram or when multiple Standards are selected. A faster processor will also help.

Why isn’t the Catalog of Recommendations available in Questions mode on the Standards screen?

The Catalog of Recommendations, Version 7 was the foundation for the Universal Questions and so to select it would be to double-select the same set of questions. To avoid confusion, it is not selectable in Questions mode.

What Standard should I use?

Only the user can answer that question for his or her organization; however, extensive help information can be found by reviewing the Cybersecurity Standard Selection help section. The user may also consult the User Guide available from the Home screen. For a brief description of the available Standards, see the ACET Standards and Question Groupings help section.

Can I unclick an answer in the Questions screen after making a selection?

Yes. Simply click the radio button again to clear it.

ACET Revision History

Document Revision	Date	Change Description
9.0.1	April 2019	First ACET release. The user guide's base is the CSET 9.0 guide. Added Module Builder for creating custom question/requirement sets. Added standard NIST 800-53 R5 and ACET standard. Added DRL, IRP, Cybersecurity Maturity, Administration, and ACET Dashboard instructions.
9.0.3	September 2019	First release with full upgrade support
9.0.4	September 2019	First public release candidate

Overview

The Automated Cybersecurity Evaluation Toolbox (ACET) provides a repeatable, measurable and transparent process that improves and standardizes our supervision related to cybersecurity in all federally insured credit unions. ACET is a software tool for performing cybersecurity assessments of an organization's enterprise and industrial control cyber systems. It was designed to help asset owners identify vulnerabilities and improve the organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements and best practices. The presented requirement questionnaires are based on selected industry standards, common requirements, and the network diagram (or network topology and architecture).

ACET Framework

The underlying framework for ACET includes:

- Analysis and user interface tools to assist in the evaluation of an institution's Financial Information Systems (FIS), Industrial Control Systems (ICS), or other Information Technologies(IT),
- A knowledge base of cybersecurity requirements, regulations, and practices, and
- A collection of solutions to help mitigate vulnerabilities.

Basic Evaluation Process

Form the Assessment Team

Prior to beginning the assessment, form a subject matter expert team. Teams typically include representation from senior management, business, operations, IT, ICS, and security. The assembled team is responsible for determining the evaluation levels and answering specific, detailed questions on the control system and security configuration.

Familiarity with the tool will improve and speed up the assessment process. Anyone in the organization who has had training or experience with the tool should be included on the team. Alternately, the primary user should spend some time using the tool with test-only or dummy data prior to commencement of the team activity.

Documents that may be referenced should be gathered prior to the assessment. Useful reference materials include information relating to operations, maintenance, physical security, cybersecurity, and hazardous materials.

Register for an ACET Account

Register for ACET by first installing ACET. The ACET installation will be on your local desktop. If it is installed locally click the icon to start, if your ACET installation is an Enterprise or company installation see your company ACET administrator for the URL.

After installation navigate to the ACET home page. Below the login is a link that says "Register New User Account". See more on registering a new account at Register a User Account. A new assessment can be started from the user's landing page by clicking the "Start New Assessment" button.

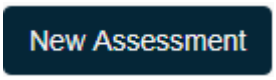


Figure: New Assessment button

Add Site Information

Begin the assessment by filling out assessment details. This includes the assessment name and date, information on the subject system, points of contact, and a description of the assessment. Such information will be helpful when referring to the assessment months or years later.

For more information, see the Assessment Details help section.

The figure below graphically depicts the next steps of the self-assessment process. A brief summary of the steps is provided below.

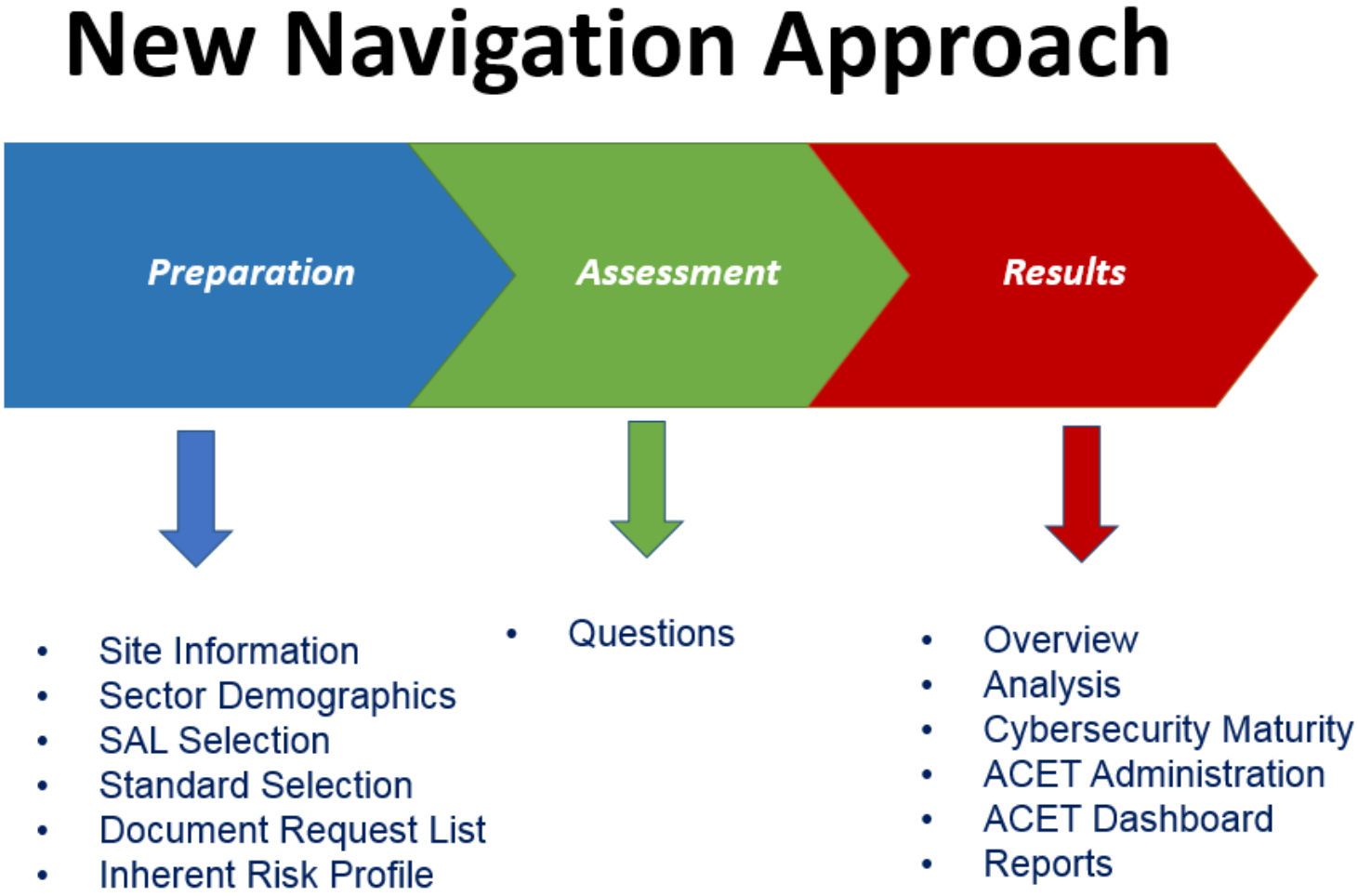


Figure: ACET Process

Preparation

Site Information

The first part of the assessment preparation process is to provide specific information about the assessment including who was responsible, when it occurred, what sites or facilities were involved, and both descriptive and summary information.

Sector Demographics

ACET collects sector and demographic information to help the user identify the appropriate Standards and questions that will be presented on the assessment.

Diagram Components

Not supported in ACET 10.2. This feature will be available in a future release.

SAL Selection

The system requires that the user identify a security assurance level (SAL), and multiple options are provided to determine what the SAL should be. The user may bypass the guidance screens and directly select the SAL.

The user may employ the General SAL guidance (consequence based) or the Federal Information Processing Standard (FIPS) 199 SAL guidance (based on FIPS 199 and National Institute of Standards and Technology (NIST), Special Publication (SP) 800-60).

The SAL value selected will limit the required questions to only those related to the selected level. The SAL value is also used in the ranking of missed questions.

For more information about Security Assurance Levels or SALs, see the Security Assurance Level (SAL) Selection help section.

Standard Selection
ACET defaults to the Automated Cybersecurity Examination Tool (found under the Financial category on the Cybersecurity Standard Selection screen).

Included on the Cybersecurity Standard Selection screen is a list of Standards and guides applicable to the mode options. The list of choices will vary depending on which mode is selected. Advanced users will have the option to select one or more Standards against which they would like to be evaluated.

For more information about Standards, see the Standards Screen help section.

Documents Request List
The Document Request List (DRL) collects the information necessary to complete the ACET.

For more information about the DRL, see the Document Request List help section.

Inherent Risk Profile
The Inherent Risk Profile (IRP) identifies an institution's inherent risk relevant to cyber risks.

For more information about the IRP, see the Inherent Risk Profiles help section.

Assessment

Questions
Once a Standard has been selected, ACET will generate a set of assessment questions that can be accessed from the Assessment screen. All questions will be answered as either Yes, No, Not Applicable (NA), or through an Alternate method (ALT). If the "Requirements" mode is selected, the questions will be presented as explicit requirements from the selected industry Standard.

The process of answering questions is tedious but straightforward. As a team, start with Question 1 and continue through each subject area or category until all questions have been discussed and answered.

Mode Selection
There are two different methods to performing an assessment. The first uses a set of simplified Yes or No questions that have been extracted from industry Standards. These questions do not combine multiple concepts; rather, they address a single idea with each question.

The second mode presents the specific requirement text directly from the selected industry Standards. This requirement mode is designed for regulated industries where the exact wording is important.

For more information, see Mode Selection.

Results

Dashboard

The Results dashboard shows the basic score or results of the assessment at a glance. The overview shows 2 scores: (1) the overall score, and (2) a standards based score. It also shows charts for Assessment Compliance, Top Ranked Categories, Standards Summary, and Component Summary.

Analysis
Assessment results can be reviewed in two locations. The first is from the Analysis Screen containing charts and tabular data that present both summary and detailed information about how well users are doing and where they need to improve, including rankings for questions by category and the questions themselves.

The second way to view assessment results is through a set of printed reports. From the executive to the site summary and the site detail reports, each report provides increasing levels of detail. Finally, the security plan report provides a template for documenting the required cybersecurity controls and the degree to which they are met. The printable reports contain charts, lists, and detail information found on the analysis screen.

For more information about Analysis, see the Results help section.

ACET Information
The ACET Information portion of the Results tab includes the Cybersecurity Maturity table, Administration information, and the ACET dashboard.

For more information about ACET analysis and reports, see the ACET Information help section.

Reports
The reports provide the details and scores of the assessment and allow for printing and publishing the assessment information, including summary charts and lists. Reports can help the user clearly understand where weaknesses are and where improvements should be made.

Additional Actions

Utilize Assessment Documents

ACET gives users the opportunity to collect and store all documents relevant to an assessment. This collection may be accomplished in two ways. First, all questions can have one or more documents associated with them indicated in the documents section of the details and resources link under each question. The second way is accessed from the Assessment Documents link accessed from the Help menu. The Document Library screen lists all documents currently associated with the assessment.

For more information, see the Assessment Documents help section.

Utilize Resource Library

The Resource Library is a source for additional cybersecurity documentation. It is accessed from the Title Bar on the main ACET window. The Resource Library contains reference materials to answer many technical or policy questions and aid in the creation and maintenance of a comprehensive cybersecurity program.

For more information, see the Resource Library help section.

Protect Information

Data Recovery

ACET continuously saves data that is entered. If ACET is closed or the browser restarts all the entered data should remain.