

ACET

AUTOMATED CYBERSECURITY EVALUATION TOOLBOX



National Credit
Union Administration

USER MANUAL

Automated Cybersecurity Evaluation Toolbox(ACET), Version 10.3.1.

User Manual

August 2021

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

Table of Contents

| | |
|--------------------------------------|----|
| Introduction to ACET | 4 |
| Introduction..... | 5 |
| Disclaimer..... | 7 |
| System Basics | 8 |
| System Requirements..... | 9 |
| Installation Procedure..... | 10 |
| Using the Stand-alone | 16 |
| Evaluation Preparation | 18 |
| Register a User Account | 20 |
| Import/Export a ACET Assessment..... | 22 |
| Importing a .acet File..... | 23 |
| Exporting an ACET Assessment..... | 24 |
| Title Bar..... | 25 |
| Tools Menu | 27 |
| Parameter Editor | 29 |
| Export to Excel..... | 31 |
| Export ACET to Excel | 32 |
| Import Module | 33 |
| Module Builder..... | 36 |
| Create a New Module | 37 |
| Add Requirements..... | 39 |
| Add Questions | 43 |
| Manage Documents | 46 |
| Resource Library..... | 48 |
| Search Screen..... | 49 |
| Browse Screen..... | 51 |
| Help Menu | 55 |
| Accessibility Document..... | 57 |
| Keyboard Shortcuts | 58 |
| Terms of Use | 59 |
| About ACET..... | 60 |
| Advisory..... | 61 |
| User Profile | 62 |
| User Profile..... | 63 |
| Change Password | 64 |
| Operation Menus..... | 65 |
| Prepare Menu | 66 |
| Statements Menu..... | 68 |
| Results Menu | 70 |
| Main ACET Window Sections | 72 |
| Prepare Section..... | 73 |
| ACET Landing Page | 74 |
| Assessment Configuration..... | 76 |
| Assessment Information | 78 |
| Inherent Risk Profiles | 80 |
| Inherent Risk Profile Summary..... | 83 |

| | |
|--|-----|
| Assessment Section..... | 84 |
| Assessment Screen | 85 |
| Statement Details, Resources, and Comments | 87 |
| Exam Step..... | 90 |
| Supplemental Section | 91 |
| Comments Section | 92 |
| References Section | 93 |
| Observations Section..... | 94 |
| Statement Observations | 95 |
| Statements Filter..... | 98 |
| Results Section..... | 100 |
| ACET Maturity Results..... | 101 |
| ACET Dashboard..... | 104 |
| Reports Section..... | 106 |
| Report Screen | 107 |
| Executive Summary..... | 109 |
| Gap | 110 |
| Comments and Marked for Review | 111 |
| Answered Statements | 112 |
| Compensating Controls | 113 |
| Glossary | 114 |
| ACET Revision History | 117 |

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 ACET Maturity Assessment is an assessment of a Credit Union's Inherent Risk and Cybersecurity Maturity. The ACET provides the National Credit Union Administration (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 Federal Financial Institutions Examination Council (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 evaluate 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 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, 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.

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 before 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 website 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 isn't 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”.

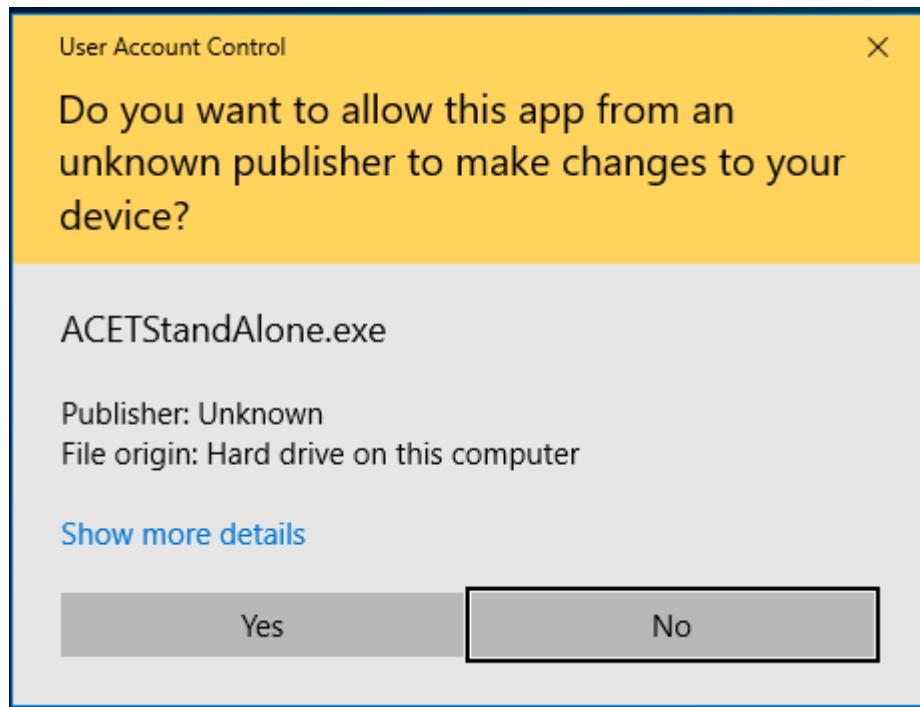


Figure: User Account Control box

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

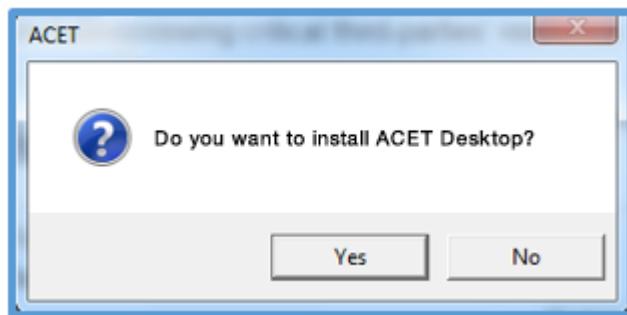


Figure: Install dialogue

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".

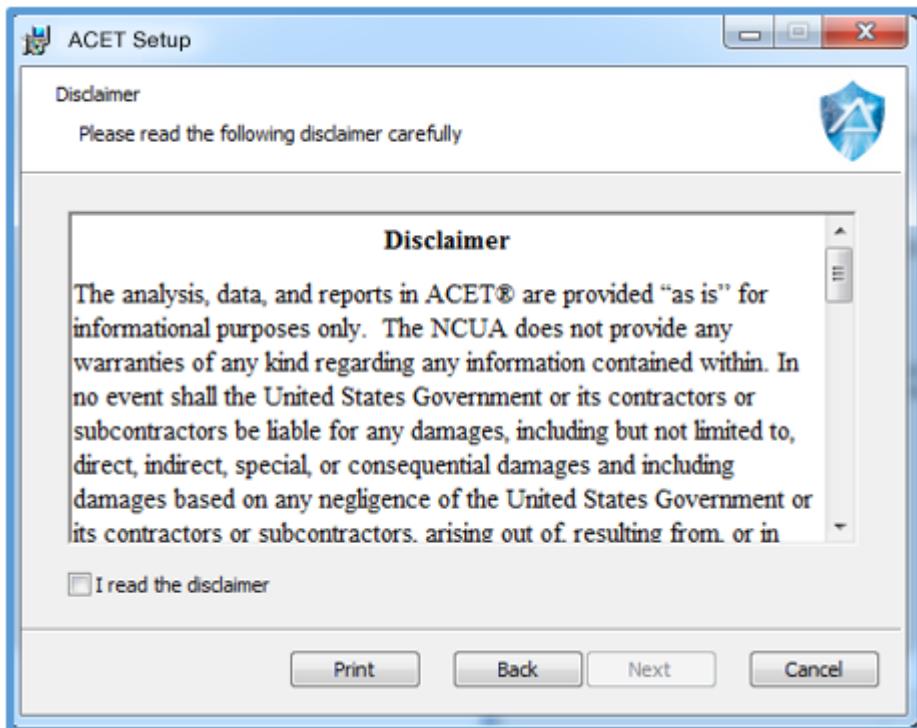


Figure: ACET Setup

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".

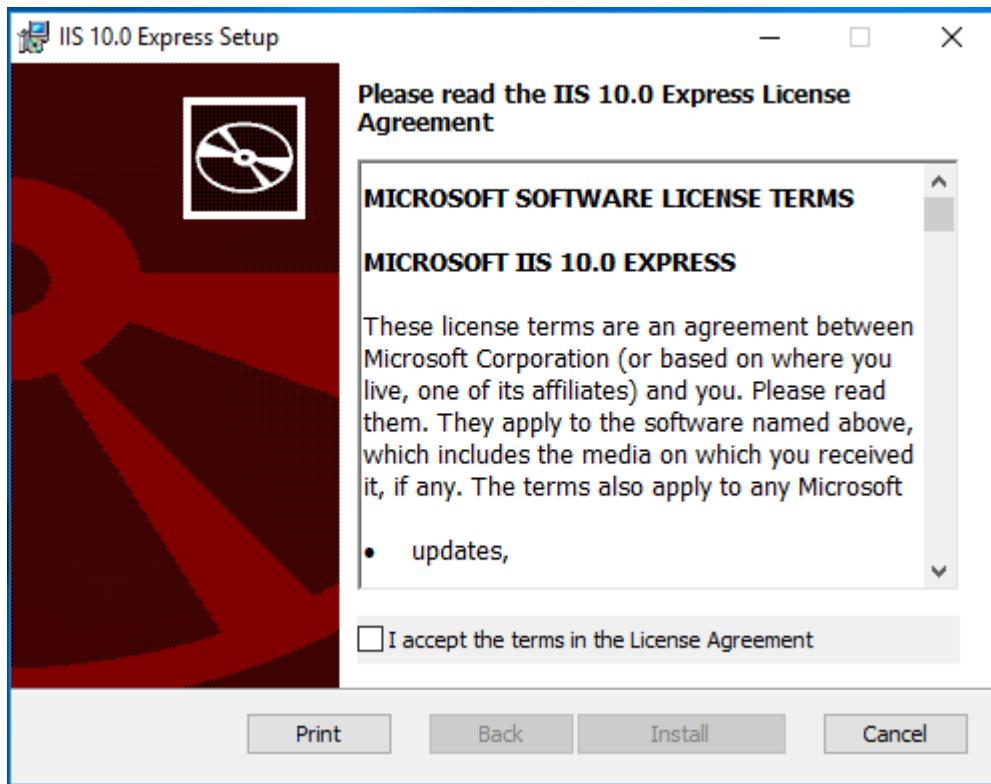


Figure: IIS Setup

IIS will install. Select "Finish" when it completes.

The ACET Setup Wizard will open to walk the user through the install process. Select "Next".

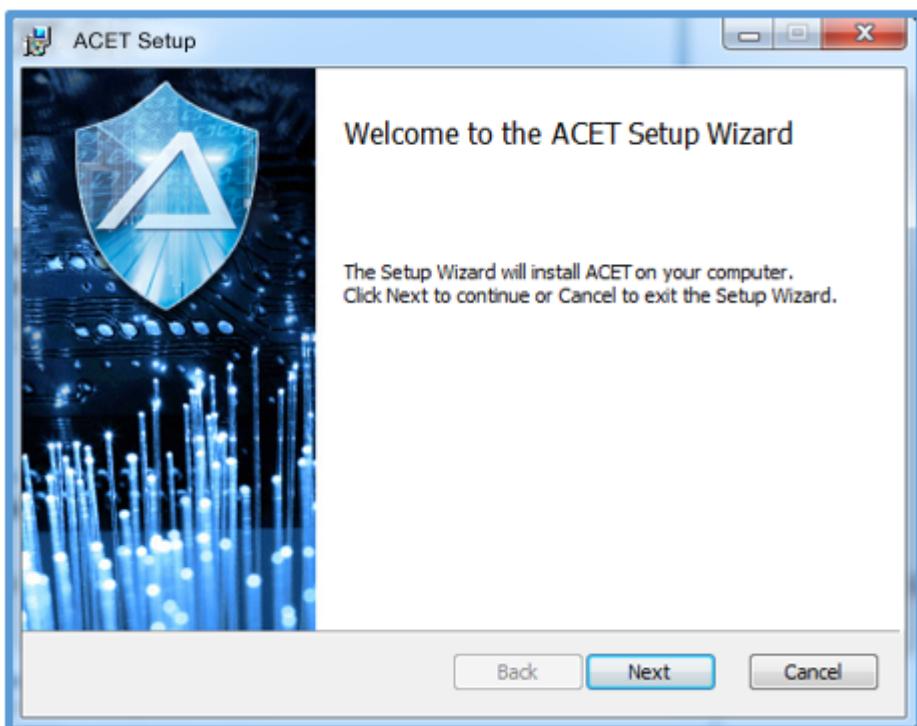


Figure: Setup Wizard

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

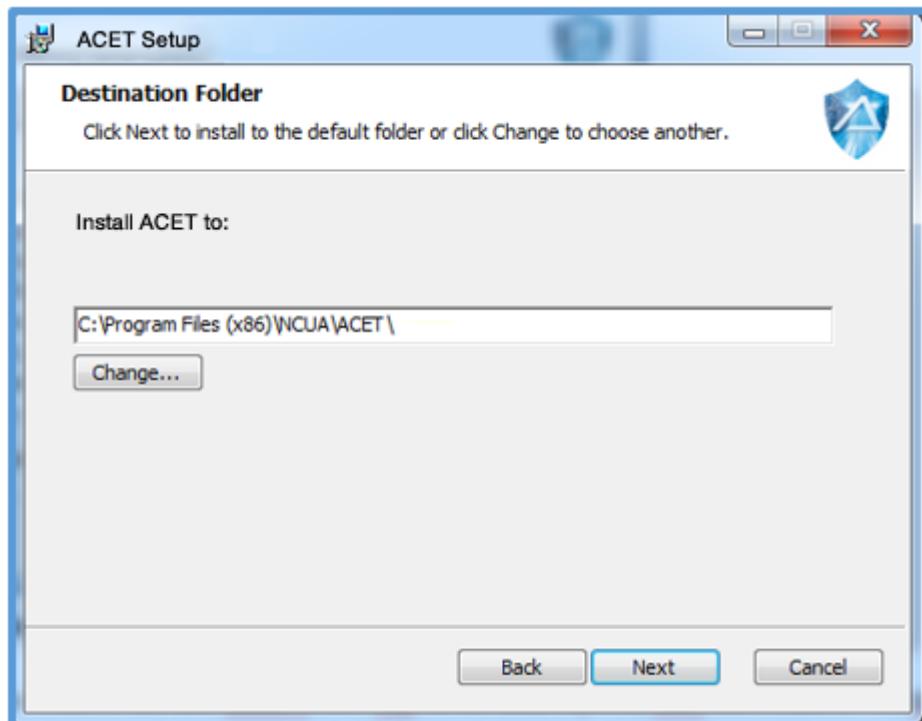


Figure: Destination Folder

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

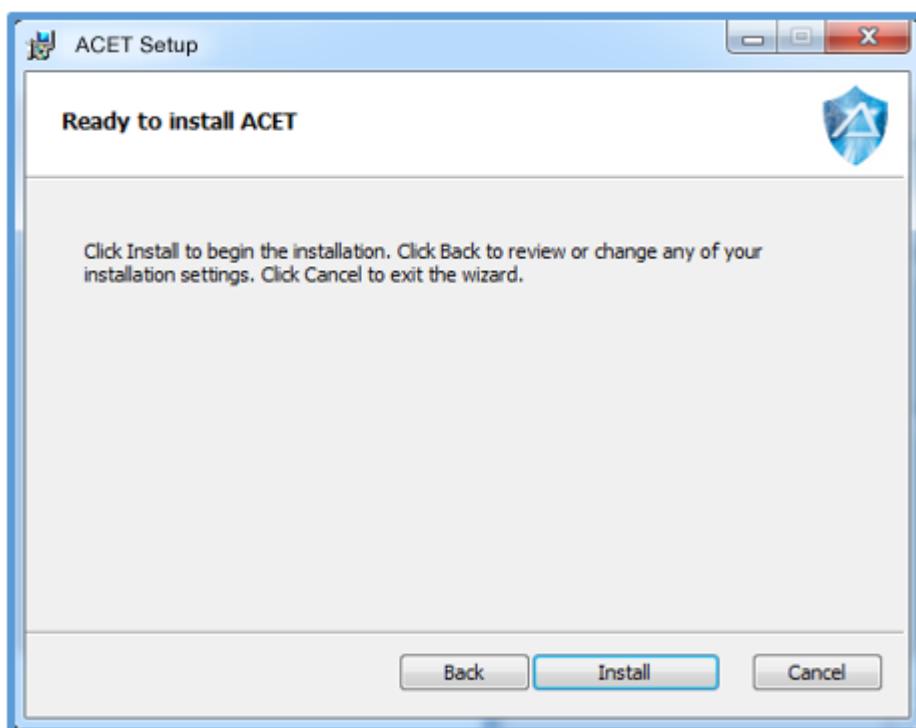


Figure: Ready to Install

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.

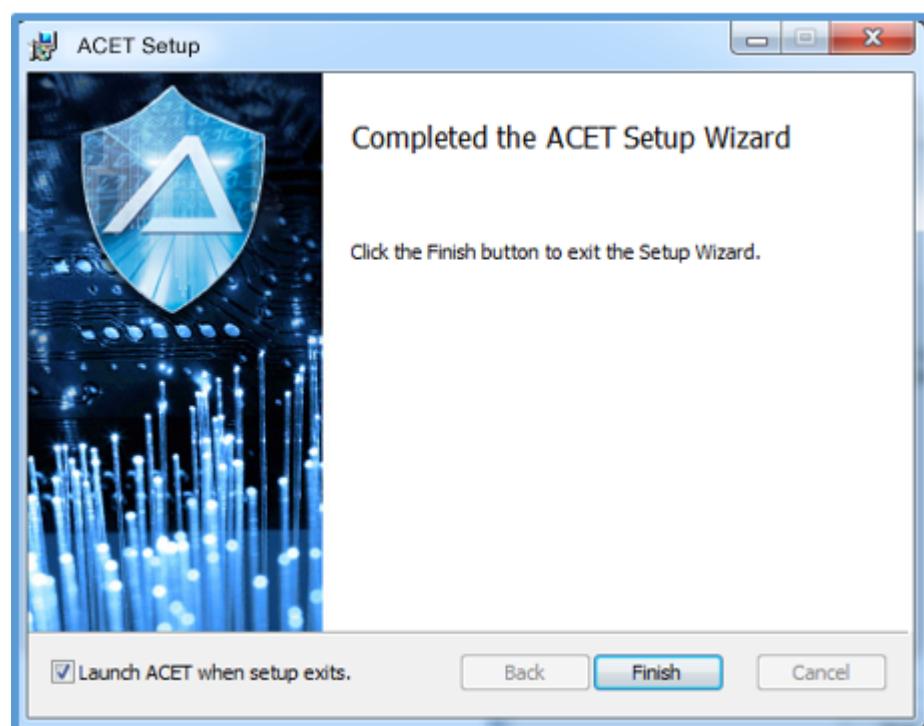


Figure: Setup Successful

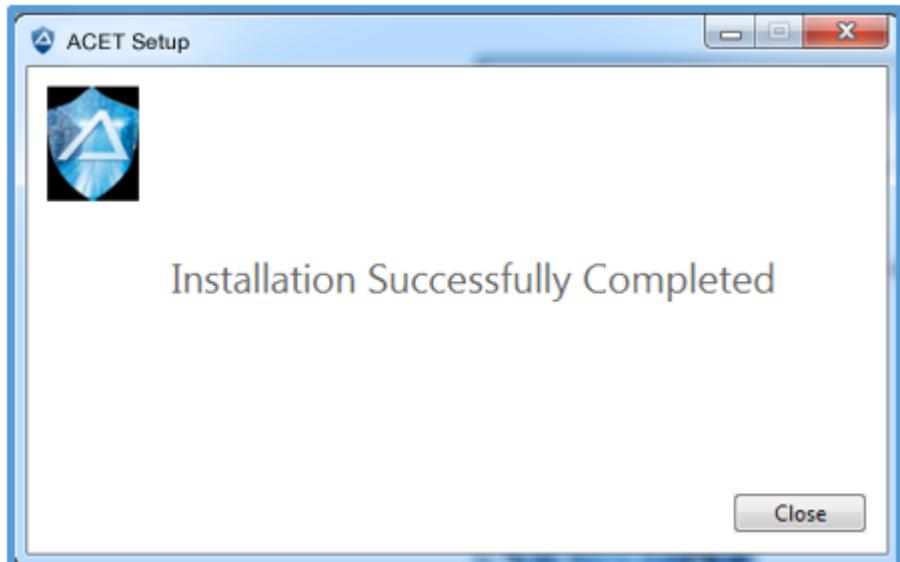


Figure: Installation Successful

After getting this message restart your machine.

The user 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.

A screenshot of the ACET Local Installation landing page. The top navigation bar is blue, featuring the "Local Installation" tab, the ACET logo, a "Tools" dropdown, and a user profile for "WHITMJ". The main content area has a white background. At the top left, it says "Welcome to ACET". Below that, a message reads: "To get started, select from one of the options below:". There are two prominent buttons: a dark blue button on the left labeled "Start a New Assessment" with a shield icon, and a light gray button on the right labeled "Import an Existing Assessment" with a downward arrow icon. A descriptive paragraph at the bottom explains the tool's purpose: "The Automated Cybersecurity Examination Toolkit (ACET®) is a National Credit Union Administration (NCUA) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the National Credit Union Administration by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems." A small upward-pointing arrow is located at the very bottom center of the page.

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 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.

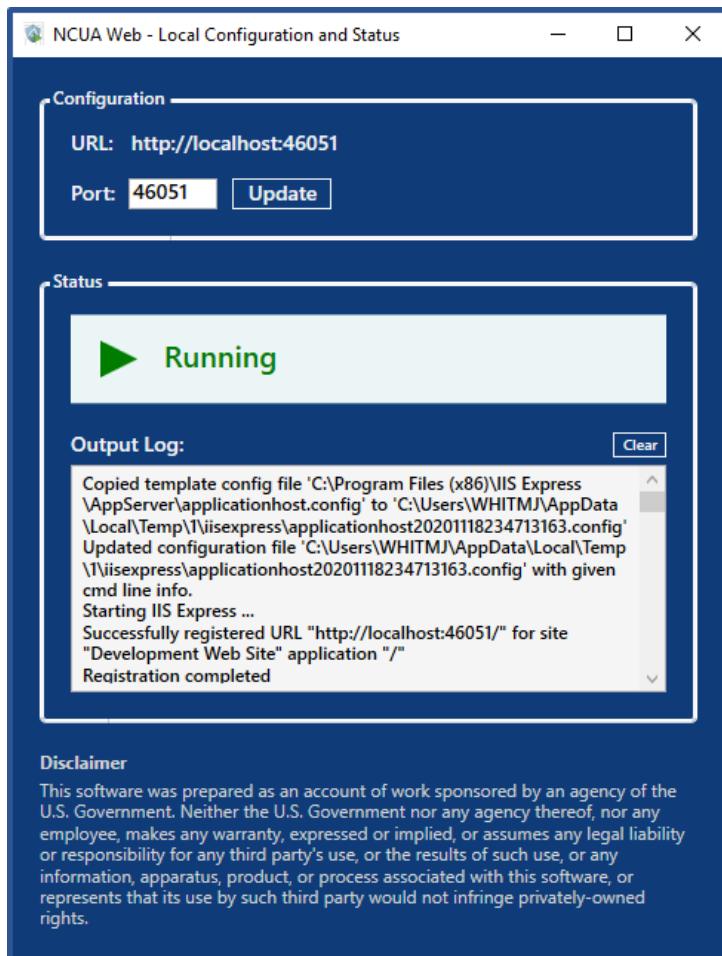


Figure: Local Configuration and Status box

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 username displayed as their name.

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

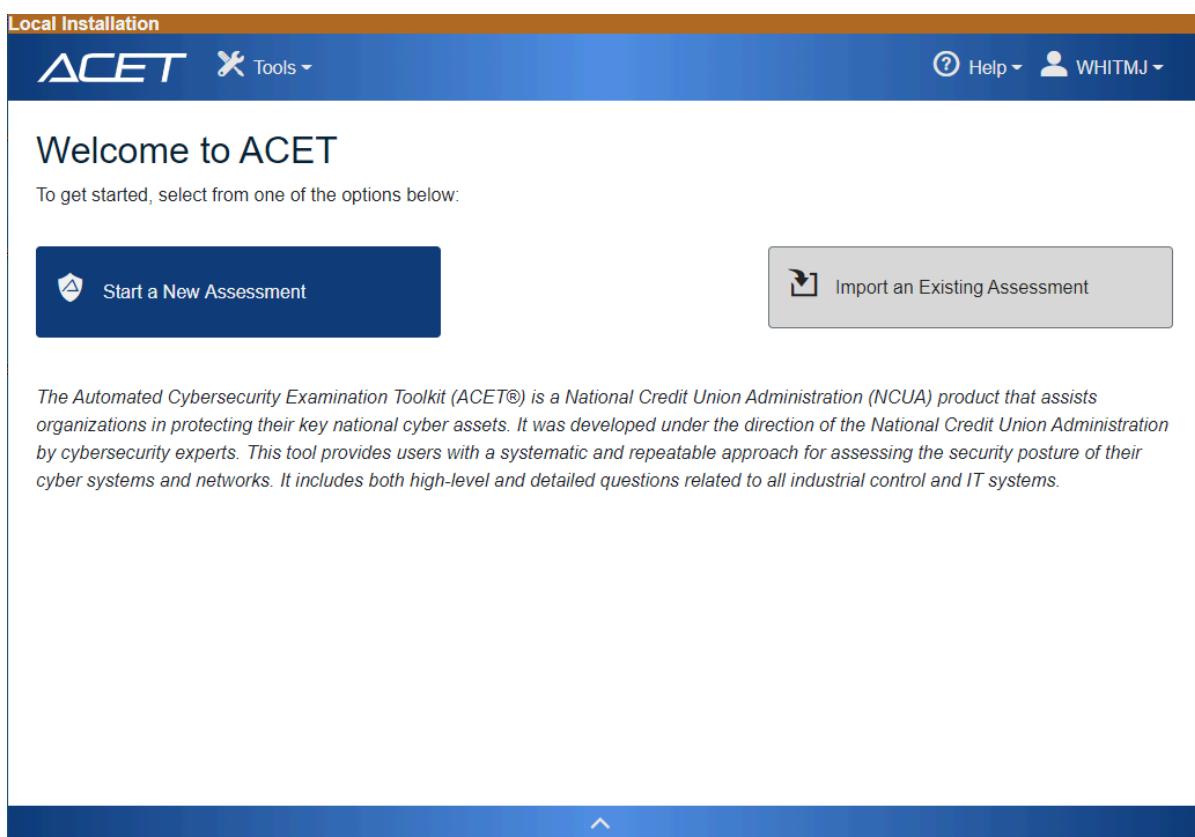


Figure: Stand-alone Landing page

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).

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 may be provided by your company's ACET administrator.

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

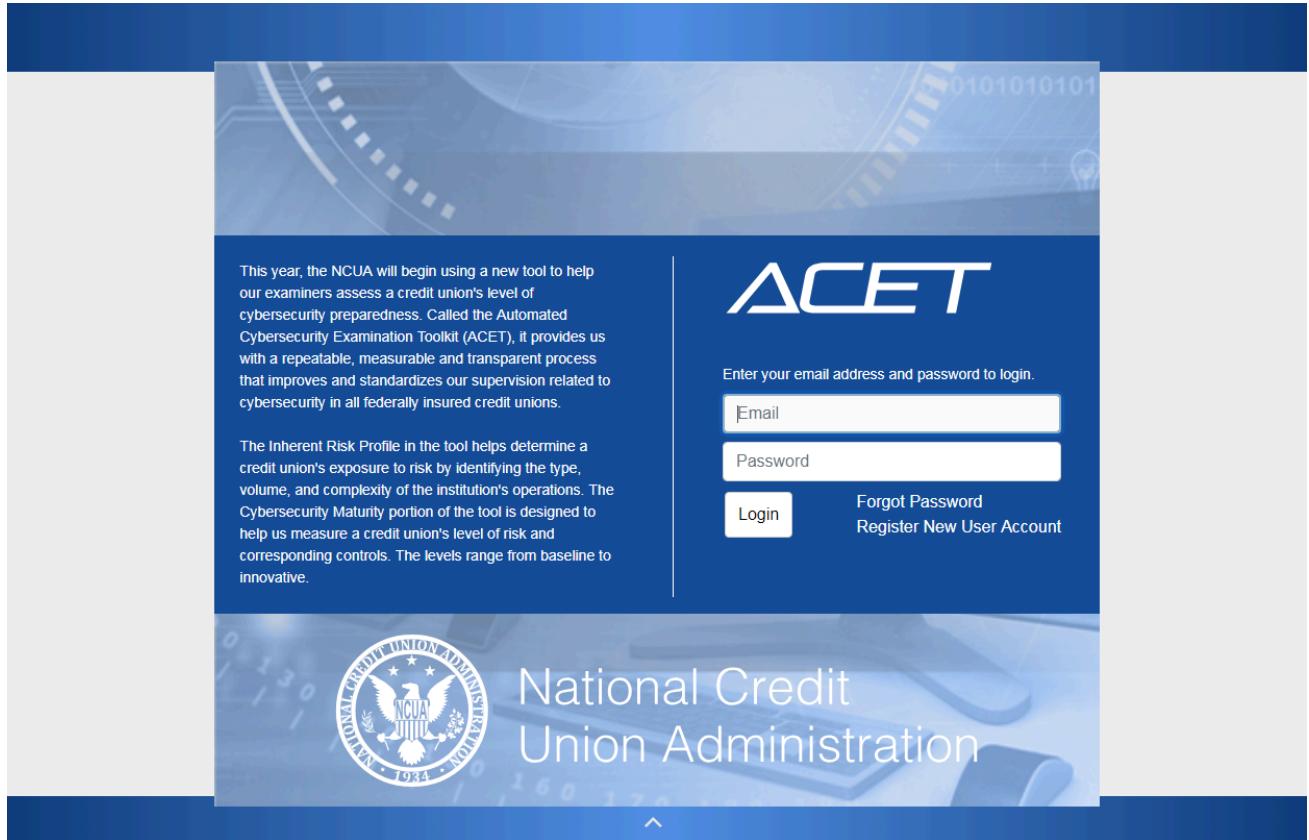


Figure: ACET Home Screen

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.

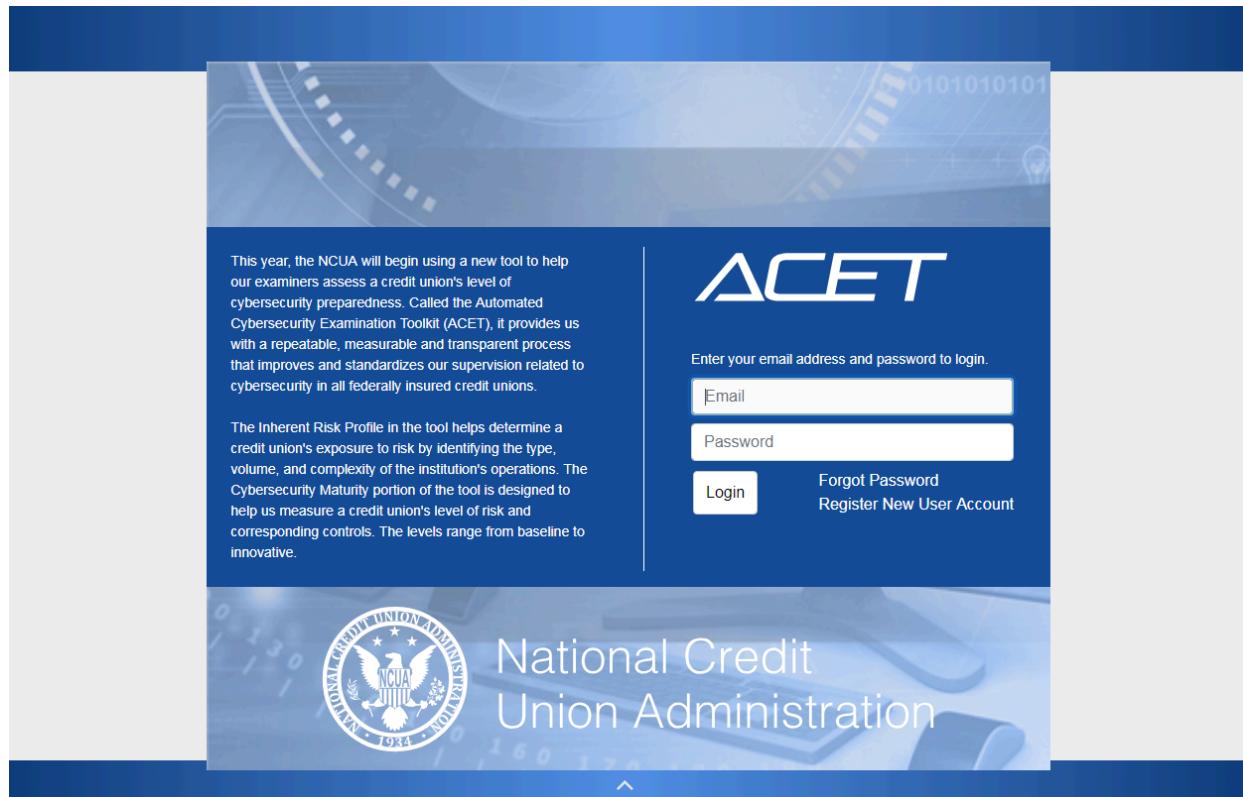


Figure: Using the Home page to register an account

1 Login Email and Password fields

Email

Password

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

2 Forgot Password link

[Forgot Password](#)

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

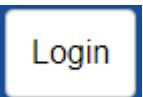
3 Register Account link

[Register New User Account](#)

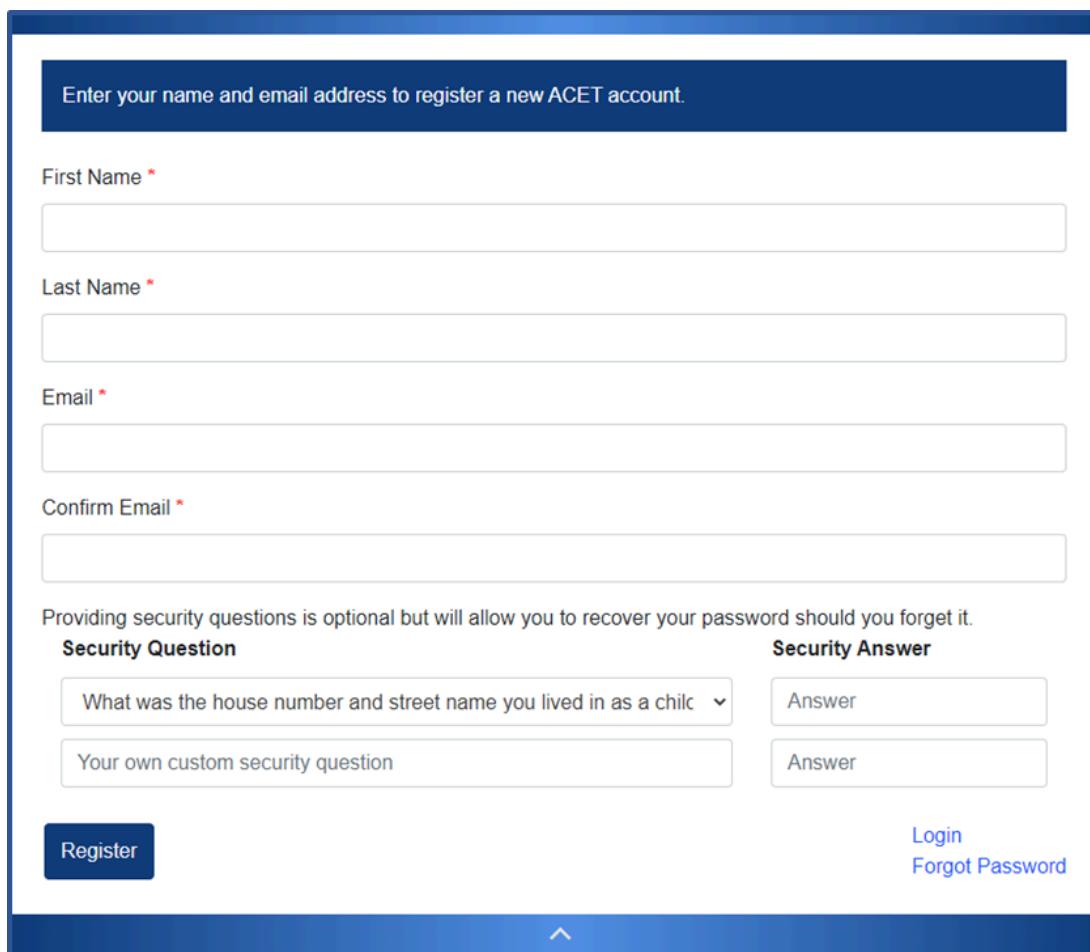
This link will open a dialogue for the user to create a new account.

4

Login button

A blue rectangular button with the word "Login" in white text.

Click the login button after entering user information to login.



The screenshot shows a registration form with the following fields:

- A header message: "Enter your name and email address to register a new ACET account."
- "First Name *": An input field.
- "Last Name *": An input field.
- "Email *": An input field.
- "Confirm Email *": An input field.
- A note: "Providing security questions is optional but will allow you to recover your password should you forget it."
- "Security Question" section:
 - A dropdown menu: "What was the house number and street name you lived in as a child"
 - An "Answer" input field.
- "Your own custom security question" input field.
- "Answer" input field.
- "Register" button (blue).
- "Forgot Password" link (blue).

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.

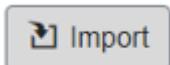


Figure: Import Button

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 on 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.

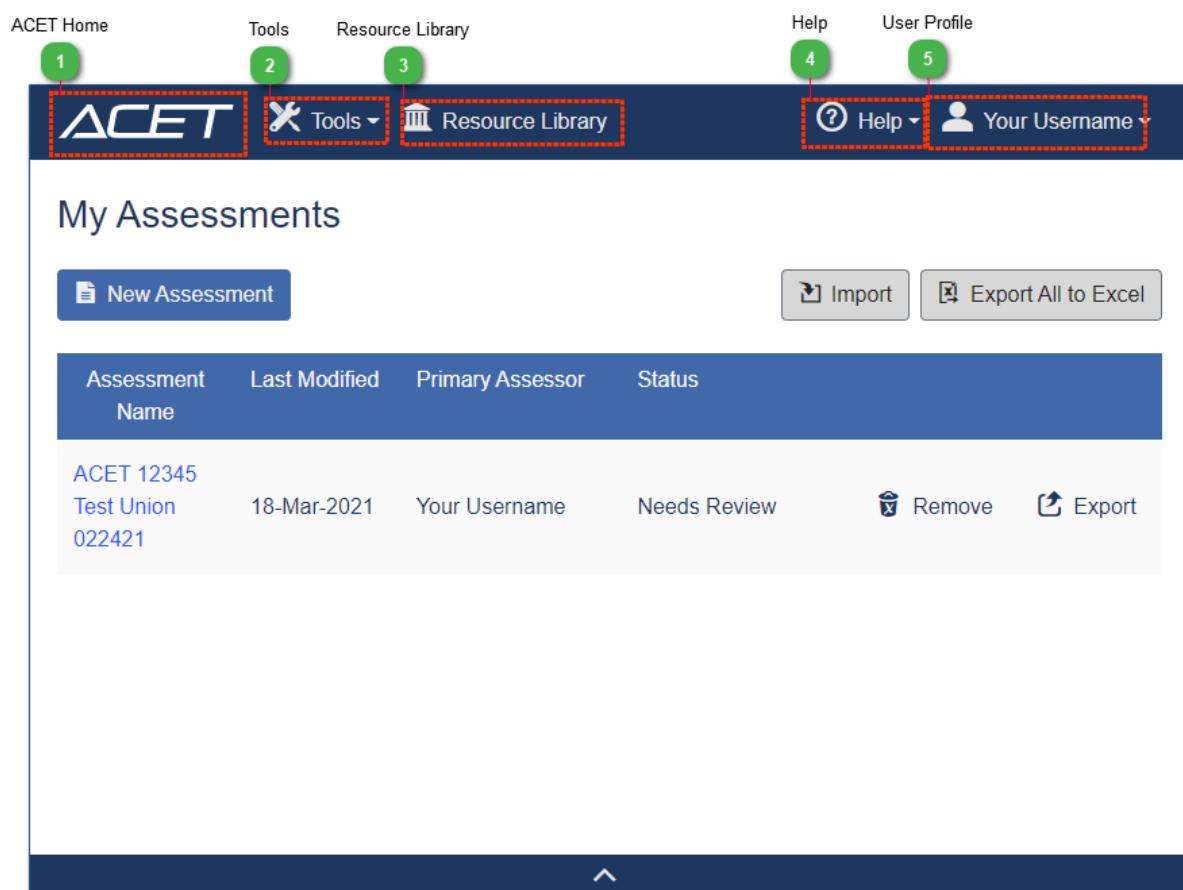


Figure: Title Bar



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

For more information about the landing page, see the [Landing Page](#) help section.



The Tools button opens the Tools menu.

For more information about the Tools menu, see the [Tools Menu](#) help section.

3 Resource Library



The Resource Library opens the Resource Library in a new tab.

For more information about the Resource Library, see the [Resource Library](#) help section.

4 Help



The Help button opens the Help menu.

For more information about the Help menu, see the [Help Menu](#) section.

5 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.

Tools Menu

The Tools Menu provides you with options outside of the assessment process. You can access the Enable Protected Features, Parameter Editor, Export Assessment to Excel, Export ACET to Excel, Export All ACET to Excel, Import Modules and Module Builder. The Tools Menu is described in the figure below.

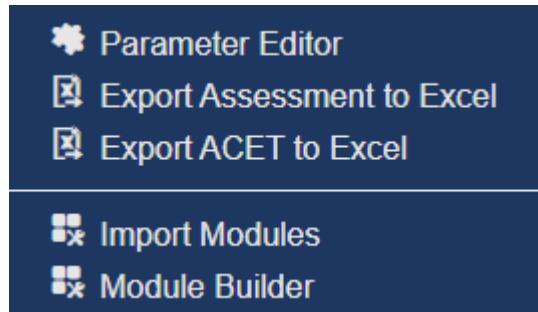


Figure: Tools Menu

Click the Tools menu button to open the Tools menu.

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](#) for 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.

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

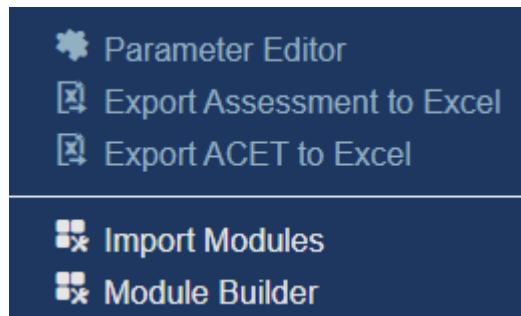


Figure: Tools menu outside of an assessment

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 on the parameter edit and save.

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

The screenshot shows a software window titled "Parameter Editor". The title bar includes a gear icon and the window title. Below the title bar is a descriptive text block explaining the purpose of the editor: "Many Standards in 'Requirements Mode' contain parameters that you can change to match your specific situation. The table below allows you to change the parameter values for the indicated parameter names in this Assessment by clicking on the Default Parameter Value. Changing a default parameter value will update all related parameter values in the requirement text of the currently selected Cybersecurity Standard(s)." A table follows, with two columns: "Parameter Name" and "Default Parameter Value". The "Parameter Name" column lists several parameters with their original text in blue. The "Default Parameter Value" column shows the same text, but the first one is highlighted with a blue border, indicating it is selected or being edited. At the bottom left is an "OK" button.

| Parameter Name | Default Parameter Value |
|---|---|
| [Assignment: organization-defined time period] | [Assignment: organization-defined time period] |
| [Assignment: organization-defined frequency] | [Assignment: organization-defined frequency] |
| [Assignment: organization-defined types of digital and non-digital media] | [Assignment: organization-defined types of digital and non-digital media] |
| [Assignment: organization-defined security measures] | [Assignment: organization-defined security measures] |
| [Assignment: organization-defined list of information system components] | [Assignment: organization-defined list of information system components] |

OK

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.

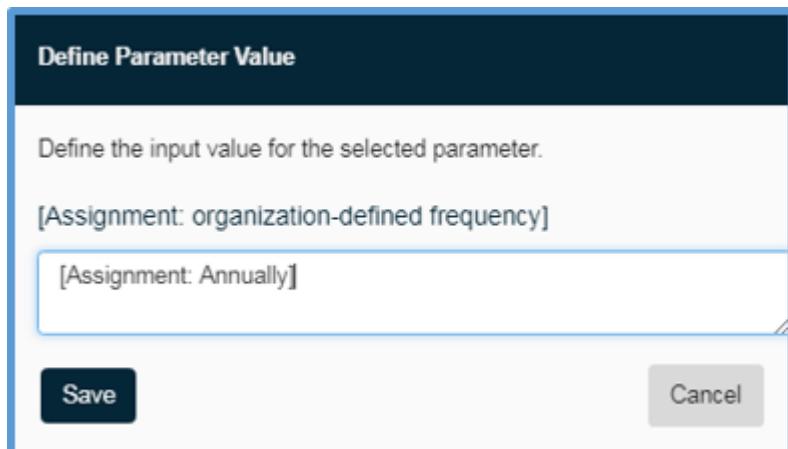


Figure: Inline Parameter Editing

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 |
|-------------|----------------------------------|--|-------------|-----------------|-------------|----------------|--------------|--------------|--------------|-----------|---------|-------------------------|-------|
| 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 |
| 1 | | 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. | | | | | | | | | | | |
| 2 | 6223 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 | 38360 | | | |
| 3 | 6224 Policies Procedures General | The facility should identify and document systems boundaries (i.e., the electronic perimeter) and has implemented security controls to limit access across those boundaries. | Y | False | False | True | False | False | 0 | 38361 | | | |
| 4 | 6225 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. | N | False | False | True | False | False | 0 | 38362 | | | |
| 5 | 6226 Access Control | The facility should practice the concept of least privilege. | NA | False | False | True | False | False | 0 | 38363 | | | |
| 6 | 6227 Access Control | | 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 | |
|----|----------|------------------------------|------------|-------|--------|-----------|-------|-------|-------|-------|------|------|------|------|------|------|------|------|
| 1 | Version | Assessment Name | CU Name | CU # | Assets | IRPC1 | IRPC2 | IRPC3 | IRPC4 | IRPC5 | IRP1 | IRP2 | IRP3 | IRP4 | IRP5 | IRP6 | IRP7 | IRP8 |
| 2 | 10.2.0.0 | ACET 12345 Test Union 022421 | Test Union | 12345 | | 1 - Least | 0 | 0 | 0 | 0 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | | | | | |
| 11 | | | | | | | | | | | | | | | | | | |

Figure: Export ACET to Excel

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.

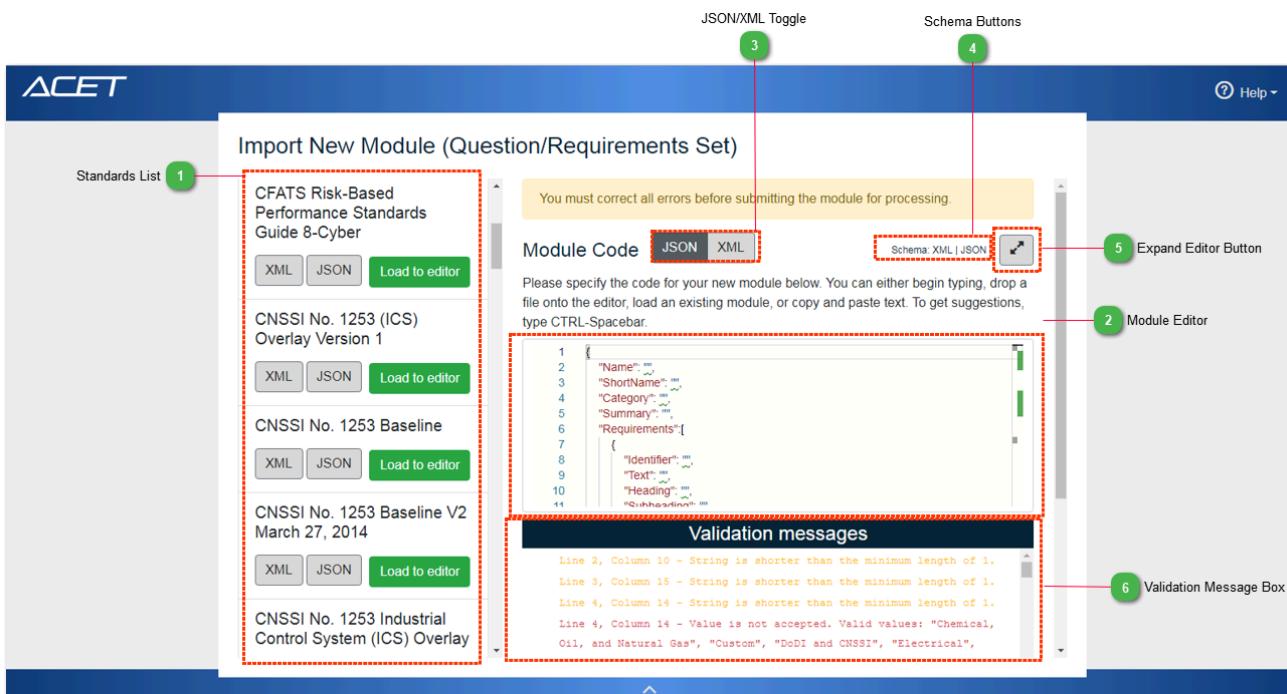


Figure: Import New Module screen

1 Standards List

- CFATS Risk-Based Performance Standards Guide 8-Cyber
 - [XML](#)
 - [JSON](#)
 - [Load to editor](#)
- CNSSI No. 1253 (ICS) Overlay Version 1
 - [XML](#)
 - [JSON](#)
 - [Load to editor](#)
- CNSSI No. 1253 Baseline
 - [XML](#)
 - [JSON](#)
 - [Load to editor](#)
- CNSSI No. 1253 Baseline V2 March 27, 2014
 - [XML](#)
 - [JSON](#)
 - [Load to editor](#)
- CNSSI No. 1253 Industrial Control System (ICS) Overlay
 - [XML](#)
 - [JSON](#)
 - [Load to editor](#)

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



```
1 {
2   "Name": "...",
3   "ShortName": "...",
4   "Category": "...",
5   "Summary": "...",
6   "Requirements": [
7     {
8       "Identifier": "...",
9       "Text": "...",
10      "Heading": "...",
11      "Subheading": "..."
12    }
13  ]
14 }
```

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

Schema: XML | JSON

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.

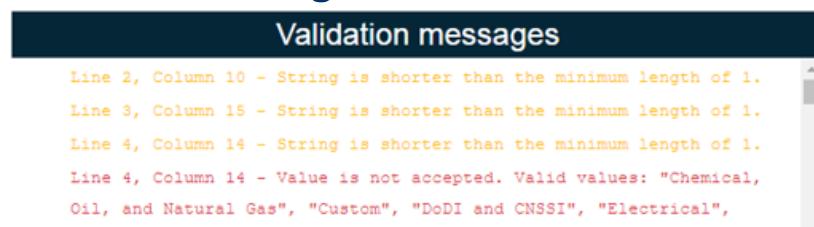
5 Expand Editor Button



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 and 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, and 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.

The screenshot shows a web-based application titled "Standard And Question Set Builder". At the top left is a "Home" link. Below the title, there is a descriptive text: "This tool allows you to define your own custom standard or question set for an assessment." A prominent blue button labeled "+ Create Module" is located on the left. To its right, three module titles are listed: "800-53 Revision 7", "Question Set 17-A", and "Branch Office Working Standard 1.7". On the far right, there are two columns of icons: "Clone" (represented by a copy symbol) and "Delete" (represented by a trash can symbol), each repeated three times.

Figure: Module list



Clone Button [Clone](#)

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 [Delete](#)

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.

The screenshot shows the ACET Module Detail screen. At the top, there is a blue header bar with the ACET logo on the left and a 'Help' dropdown on the right. Below the header, a breadcrumb navigation bar shows 'Home > Module Detail'. The main content area is titled 'Module Detail'. It contains the following fields:

- Module Name ***: A text input field containing 'USPS Cyber Standard 100.7'.
- Short Name ***: A text input field containing 'USPS Cyber 100.7'.
- Description ***: A text area containing the following text: 'USPS was created in 1775 and now has locations (post offices) all across the continental United States. Each post office is in charge of providing services to a specific jurisdiction. The United States Postal Service is governed under a number of policies and procedures established by a board of directors.'
- Category**: A dropdown menu currently set to 'Information Technology'.

At the bottom of the screen, there are three buttons: 'Requirements' (highlighted in blue), 'Questions', and 'Manage Documents'. There is also a link '« Back to Module List'.

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

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.

The screenshot shows a web-based application interface for managing requirements. At the top, there is a navigation bar with links to 'Home', 'Module Detail', and 'Requirement List'. Below this is a section titled 'Requirement Listing' with a sub-section title '800-53 Revision 7'. A descriptive text block states: 'This standard provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.' Below this, a blue button labeled '+ Create Requirement' is visible. The main content area is titled 'Access Control' and contains a sub-section 'Access Control Policy And Procedures'. Under this, a requirement is listed with the identifier 'AC-1'. The requirement details are: 'a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. An access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined senior management official] to manage the access control policy and procedures; c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the access control procedures implement the access control policy and controls; and e. Develop, document, and implement remediation actions for violations of the access control policy.' To the right of the requirement details, there are 'Edit' and 'Delete' icons.

Figure: Requirement Listing screen

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

The screenshot shows a 'Create New Requirement' dialog box. At the top left is a book icon and the text 'Add Requirement'. Below this is a descriptive note: 'Category and Subcategory are used to group Requirements in ACET. Question Group Heading and Subcategory are used to group related questions.' The form contains five input fields: 'Category' (a dropdown menu), 'Question Group Heading' (a dropdown menu with a downward arrow), 'Subcategory' (a dropdown menu), 'Title/Identifier' (a text input field), and 'Requirement Text' (a large text input field). At the bottom right are two buttons: 'Create' (in a dark blue box) and 'Cancel'.

Category and Subcategory are used to group Requirements in ACET. Question Group Heading and Subcategory are used to group related questions.

Category

Question Group Heading

Subcategory

Title/Identifier

Requirement Text

Create

Cancel

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.

Subcategory 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

Requirement Detail

| | |
|---|--------------------|
| Category | Subcategory |
| Account Management | Account Management |
| Identifier/Title * | |
| <input type="text" value="AM1"/> | |
| Standard-Specific Requirement * | |
| The organization will manage its accounts. | |
| <h3>Security Assurance Level</h3> <p>Select all applicable levels.</p> <p>Low Moderate High Very High</p> | |

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.

Supplemental Information

HTML markup can be edited directly by clicking the  button.



A rich text editor toolbar with various buttons for font style (C, B, I, U), font size (x1, x2, x3), alignment (left, center, right, justify), and other editing functions (Default, Arial, 5, A, A, %, \$, -, x, </>).

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

References

Documents that define the standard or provide additional information for the requirement are attached here. If the document is a PDF with bookmarks, entering a bookmark will create a link that will open the PDF to the target location.

To add documents to the dropdown lists, click 'Manage Documents.'

Manage Documents

Source Documents **Bookmark**

Help Documents **Bookmark**

The screenshot shows a user interface for managing references. At the top, there's a blue header bar with the title 'References'. Below it, a sub-header says 'Documents that define the standard or provide additional information for the requirement are attached here. If the document is a PDF with bookmarks, entering a bookmark will create a link that will open the PDF to the target location.' A note below that says 'To add documents to the dropdown lists, click 'Manage Documents.'' followed by a blue button labeled 'Manage Documents'. Below this, there are two sections: 'Source Documents' and 'Help Documents', each with a 'Bookmark' column. Each section has a dropdown arrow icon and a '+' button to its right. The 'Source Documents' section is currently active, showing a list of items.

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.

Related Questions

Questions may be added to the requirement. This will present a list of questions for the assessors to answer.

[+ Add Question](#)

Figure: Add Related Questions

Questions can be assigned to a Requirement 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.

Write New Question

If you wish to add a custom question to the set, enter it here.

Categorization

Question Group Heading Subcategory

--Select Heading--

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

[Add New Question](#)

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 Add New Question : 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.

The screenshot shows a search interface for finding existing questions. At the top, there is a search bar containing the text "authorization boundary" and a "Search" button with a magnifying glass icon. Below the search bar is a button labeled "Add Selected Questions". A message box indicates "8 questions were found". The results are listed in two sections, each with a question, group heading, subcategory, security assurance level, and a selection button.

Does the security plan explicitly define the authorization boundary of the system? +

Group Heading: Plans
Subcategory: Security Plan

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

Does the organization develop and document an inventory of information system components that includes all components within the authorization boundary of the information system? +

Group Heading: Configuration Management
Subcategory: Information System Component Inventory

Security Assurance Level

Select all applicable levels.

Low Moderate High Very High

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.

The screenshot shows a web-based application interface for managing standard documents. At the top, there is a breadcrumb navigation: Home > Module Detail > Manage Documents. Below this, the title "Standard Documents" is displayed, followed by the text "800-53 Revision 7". To the right, there is a blue button labeled "Import a Document" with a circular arrow icon. A "Filter" input field is present, along with a "Show Selected Items" checkbox. The main content area displays a table with two columns: "Title" and "File Name". The table contains the following data:

| Title | File Name |
|--|------------------------|
| 14 CFR 121.368 Certificate Holder | 14cfr121-368.pdf |
| 14 CFR Parts 43.11 | 14 CFR Parts 43.11.pdf |
| 14CFR Part 121.380 | 14CFR Part 121.380.pdf |
| 14CFR Part 135.439 | 14CFR Part 135.439.pdf |
| 14CFR Part 43.3 | 14CFR Part 43.3.pdf |
| 21 Steps to Improve Cyber Security of SCADA Networks_DOE | 21_Steps-SCADA.pdf |

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.

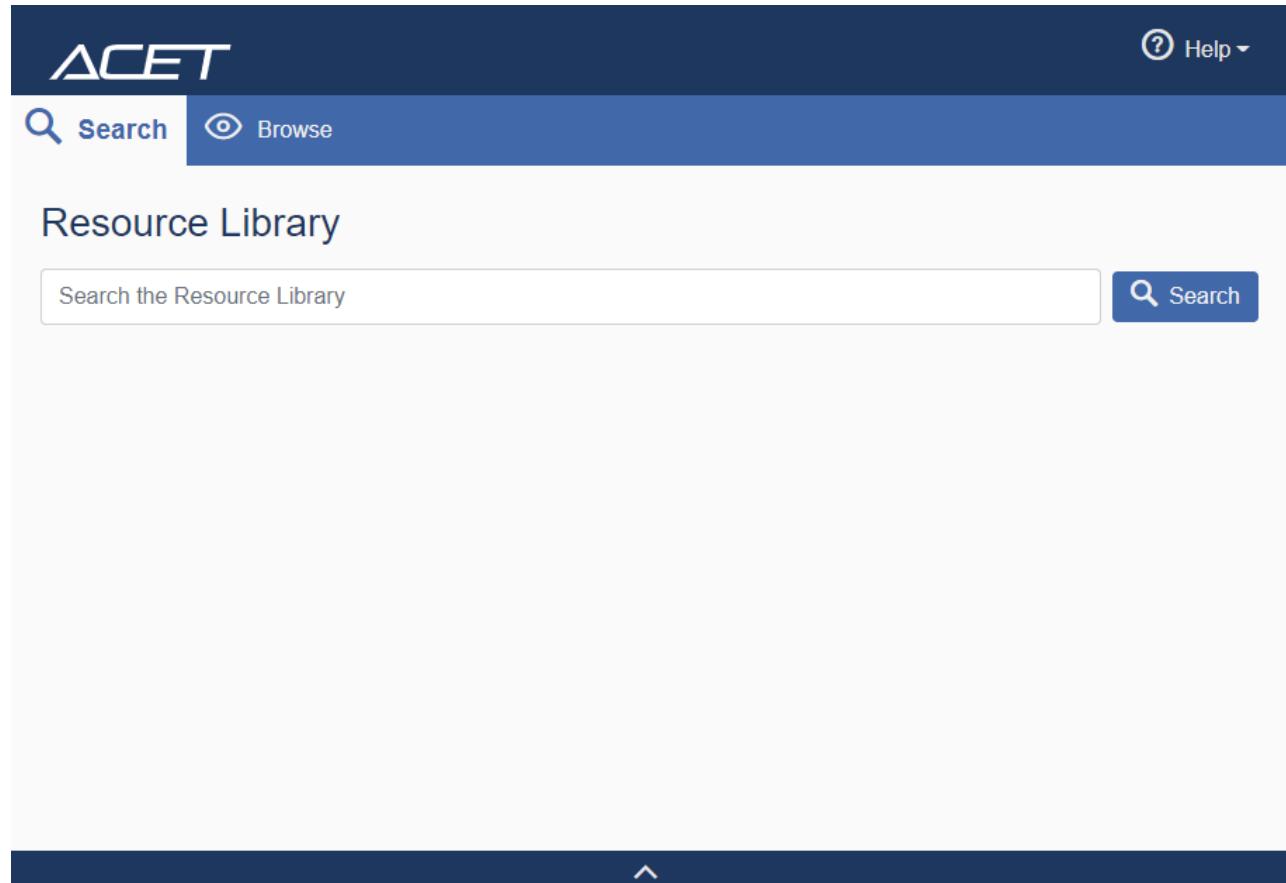


Figure: Resource Library window

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 "contingency." In this case, ACET searches through all the documents for occurrences of the word "contingency" and then ranks and presents them in an ordered list in the Search Results.

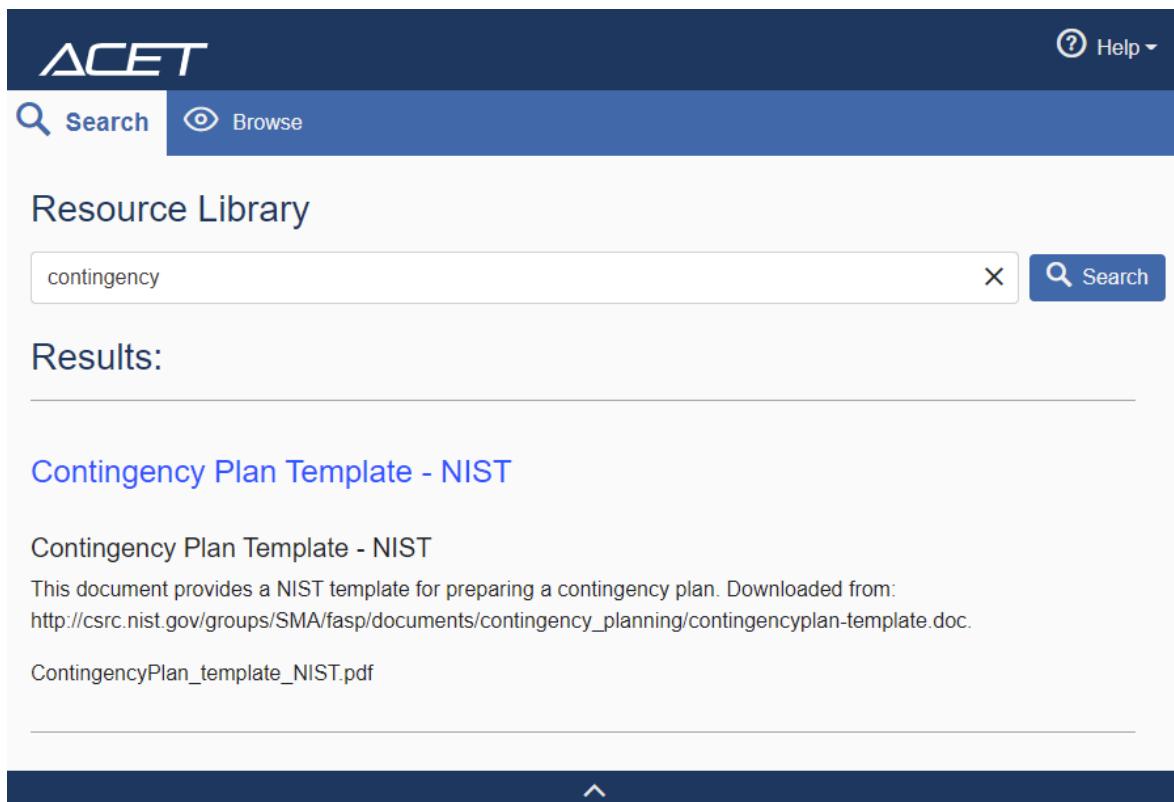


Figure: Resource Library Search screen

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

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

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.

The screenshot shows the ACET Resource Library interface. At the top, there is a dark blue header bar with the ACET logo on the left and a 'Help' button with a question mark icon on the right. Below the header is a navigation bar with a 'Search' button (magnifying glass icon) and a 'Browse' button (eye icon). The main content area is titled 'Resource Library'. It displays a hierarchical tree structure with the following branches:

- > Guidance
- > Reports
- > Templates
- > Standards
- > Publisher
- > Publication Year
- Cyber Security Procurement Language

At the bottom of the main content area, there is a dark blue footer bar with a small upward-pointing arrow icon in the center.

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.

The screenshot shows the ACET Resource Library interface. At the top, there is a dark blue header bar with the ACET logo on the left and a 'Help' button with a question mark icon on the right. Below the header is a navigation bar with two tabs: 'Search' and 'Browse'. The 'Search' tab has a magnifying glass icon, and the 'Browse' tab has a circular arrow icon. The main content area is titled 'Resource Library' in a large, bold, dark blue font. Below this title is a hierarchical menu tree. The first level includes 'Guidance', 'Reports', 'Templates', and 'Standards'. Under 'Standards', there is a collapsed icon followed by the text 'Access Control'. Below the tree, there are two document entries: 'FIPS 201-1 PIV Employees Contractors' and 'ICD 704 Personnel Controlled Access'. Each entry has a brief description and a link to the document.

FIPS 201-1 PIV Employees Contractors

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

ICD 704 Personnel Controlled Access

The directive establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs.

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).

Removal of Unnecessary Services and Programs

System hardening is a security principle that should be considered when designing and procuring control systems products. It refers to making changes to the default configuration of a Network Device and its operating system (OS), software applications, and required third-party software to limit security vulnerabilities. Removal of unnecessary services and programs is an aspect of system hardening that refers to removal of unnecessary services and programs commonly installed on network devices.

Basis

Unused services in a host operating system that are left enabled are possible entry points for exploits on the network and are generally not monitored because these services are not used. Only the services used for control systems operation and maintenance shall be enabled to limit possible entry points.

Language Guidance

Often, networked devices ship with a variety of services enabled and default operating system programs/utilities pre-installed. These range from system diagnostics to chat programs, several of which have well-known vulnerabilities. Various attacks have been crafted to exploit these services to obtain information leading to compromise the system.

Any program that offers a network service that "listens" on specific addresses for connection requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP) network, these addresses are a combination of IP address and TCP or User Datagram Protocol (UDP) ports. A recommended hardening activity is simply disabling or removing any services or programs, which are not required for normal system operation, thus removing potential vulnerabilities.

Port scans are the normal method of ensuring existence of required services and absence of unneeded services. A port scan shall be run before the FAT with a representative, fully functional system configuration. All input/output (I/O) ports need to be scanned for UDP and TCP. The scan needs to be run before the FAT and again prior to the SAT. Port scans can rarely be used on production systems. In most cases, scanners will disrupt operations.

Procurement Language

Postcontract award, the Vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the control system.

The Vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

OK

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.

Security Policy and Procedures

Security policies are an extension of higher-level organizational policies with consideration for identified risks. Procedures implement the policies and allow the organization to communicate to employees, third party contractors, and vendors how the security program will be managed.

Requirement

The organization develops, implements, and periodically reviews and updates:

1. A formal, documented, control system security policy that addresses:
 1. The purpose of the security program as it relates to protecting the organization's personnel and assets
 2. The scope of the security program as it applies to all organizational staff and third-party contractors
 3. The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization's security policy and other regulatory commitments.
2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each family contained in this document.

Supplemental Guidance

The security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the control system in particular, when required.

Requirement Enhancements

None

References

NIST Special Publication 800-53 Revision 3 AC-1, SC-14, PM-1
20 Critical Security Controls Twenty Critical Controls for Effective Cyber Defense: Consensus Audit CC-9

OK

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.

Help Menu

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

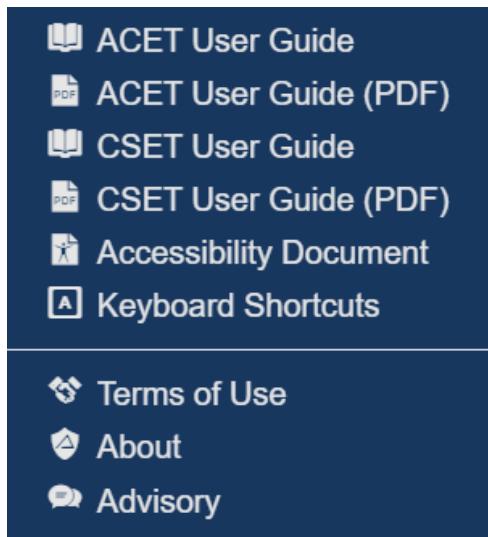


Figure: Help Menu



Click the Help menu button to open the Help menu.

ACET User Guide: Clicking the ACET User Guide menu item will open the ACET guide as a CHM file containing screenshots and instructional information for using the ACET tool.

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

CSET User Guide: Clicking the CSET User Guide menu item will open the CSET guide as a CHM file containing screenshots and instructional information for using the CSET features of this tool.

CSET User Guide (PDF): Clicking the CSET User Guide (PDF) menu item will open the CSET guide as a PDF file containing screenshots and instructional information for using the CSET features of this tool.

Accessibility Document: 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.

Keyboard Shortcuts: 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.

Terms of Use: Clicking the Terms of Use menu item will open the ACET Terms of Use that describes the terms that users agree to when using ACET.

See [Terms of Use](#) for more information.

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

See [About ACET](#) for more information.

Advisory: 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.

Accessibility Statement

In consideration of Section 508 of the U.S. Rehabilitation Act (29 U.S.C. 794d), the features and functions in this application have been developed to support users with accessibility requirements. Industry best practices and standards have guided our design and development processes to incorporate accessibility features built into the Windows operating system and the .NET architecture, as well as the Chrome, Firefox, and Edge browsers. The software development team is committed to integrating accessible design thinking throughout the entire product development cycle.

More information on Section 508 and the technical standards can be found at www.section508.gov.

If you require assistance or wish to report an issue related to the accessibility of any content on this website, please visit our [feedback page](#). If applicable, please include the web address or URL and the specific problems you have encountered.

Adobe Acrobat PDF Files

Many of the documents in this application are in HTML or ASCII (plain text) formats. These formats are generally accessible to people who use screen readers. We also have a large number of documents in Adobe Acrobat® Portable Document Format (PDF).

When using a screen reader to read documents directly in PDF format using Adobe Acrobat Reader, you will likely need to install an accessibility plug-in. This plug-in is available free of charge on the [Adobe Accessibility](#) website.

Accessibility Features

Our team works to integrate Section 508 accessibility considerations in every application update and release.

Keyboard Shortcuts

We offer app-specific keyboard shortcuts in the Help menu.

Browser Support

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.

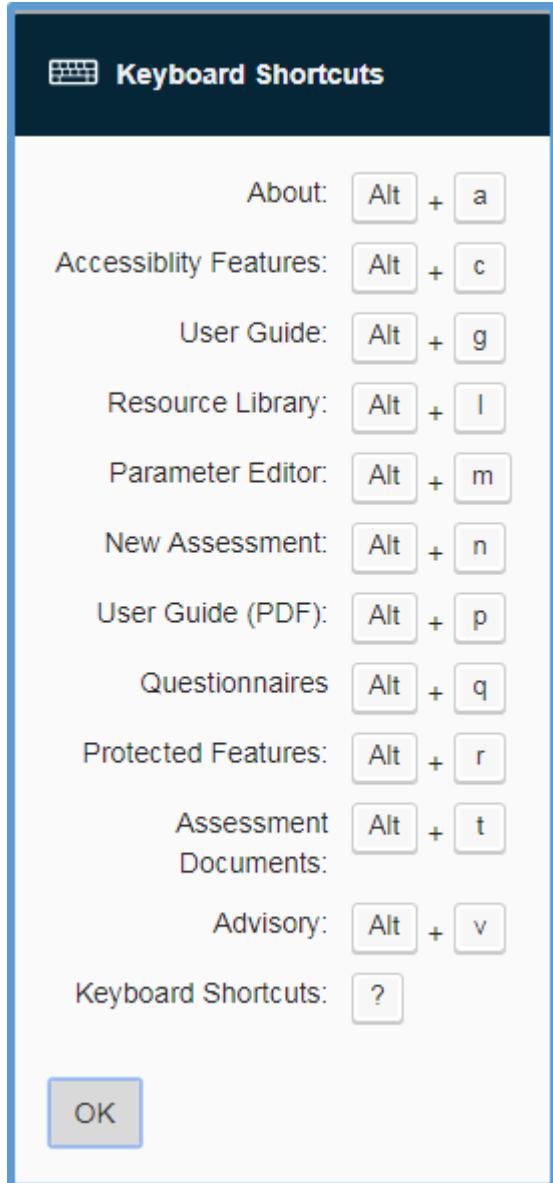


Figure: ACET Keyboard Shortcuts Document

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.

The screenshot shows a software application window titled "About". The main content area displays the "ACET" logo, the text "Automated Cybersecurity Evaluation Toolbox", the URL "<https://www.ncua.gov>", and the National Credit Union Administration logo. Below this, there is a section titled "Contact" with the text "Office of Examination and Insurance, Critical Infrastructure Division" and an email address "CU_Cybersecurity@NCUA.GOV". A large "OK" button is visible at the bottom left of the window.

ACET

Automated Cybersecurity Evaluation
Toolbox

<https://www.ncua.gov>

National Credit
Union Administration

We Ensure Financial Stability

The NCUA ensures that millions of consumers, businesses and communities can safely use federally insured credit unions for their financial needs.

OK

ACET Training Resources

ACET training is available through the following resource:

User Guide

Contact

Office of Examination and Insurance,
Critical Infrastructure Division
CU_Cybersecurity@NCUA.GOV

Figure: About ACET Window

Advisory

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

The screenshot shows a dark blue header bar with a speech bubble icon and the word "Advisory". Below this is a white content area with the following text:

Automated Cybersecurity Evaluation Toolbox

The Automated Cybersecurity Evaluation Toolbox (ACET)® is only one component of the overall cyber security picture and should be complemented with a robust cyber security program within the organization. A self-assessment with ACET® cannot reveal all types of security weaknesses, and should not be the sole means of determining an organization's security posture.

The tool will not provide a detailed architectural analysis of the network or a detailed network hardware/software configuration review. It is not a risk analysis tool so it will not generate a complex risk assessment. ACET® is not intended as a substitute for in-depth analysis of control system vulnerabilities as performed by trained professionals. Periodic onsite reviews and inspections must still be conducted using a holistic approach including facility walk-downs, interviews, and observation and examination of facility practices. Consideration should also be given to additional steps including scanning, penetration testing, and exercises on surrogate, training, or non-production systems, or systems where failures, unexpected faults, or other unexpected results will not compromise production or safety.

ACET® maturity assessments cannot be completed effectively by any one individual. A cross-functional team consisting of representatives from operational, maintenance, information technology, business, and security 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 effectively answer all the questions.

Data and reports generated by the tool should be managed securely and marked, stored, and distributed in a manner appropriate to their sensitivity.

Figure: Advisory Screen

User Profile

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

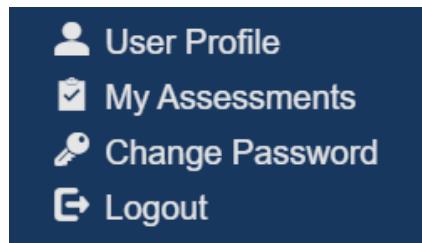


Figure: User Profile menu

Click the User Profile menu button Your Username ▾ to open the User Profile menu.

User Profile: Click User Profile to view and edit User Profile Information.

See [User Profile Information](#) for more information.

My Assessments: Click My Assessments to be directed to your Landing Page.

See ACET [Landing Page](#) for more information.

Change Password: Click Change Password to change the user's password.

See [Change Password](#) for more information.

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 you to change your First Name, Last Name, and/or Email. The menu also provides a space to choose and enter answers for security questions.

The screenshot shows the 'Edit User Profile' dialogue box. It contains fields for First Name, Last Name, and Email, each with a required asterisk. Below these are fields for Confirm Email and Security Questions. The Security Questions section includes dropdowns for 'What was the house number and street name you lived in as a child?' (selected) and 'What is your first pet's name?', and corresponding answer fields ('160 childs ave' and 'Spike'). At the bottom are 'Save' and 'Cancel' buttons.

| Edit User Profile | |
|--|-----------------|
| First Name * | Your |
| Last Name * | Username |
| Email * | |
| Confirm Email * | |
| Providing security questions is optional but will allow you to recover your password should you forget it. | |
| Security Question | Security Answer |
| What was the house number and street name you lived in as a child? | 160 childs ave |
| What is your first pet's name? | Spike |
| Save | Cancel |

Figure: Edit User Profile dialogue

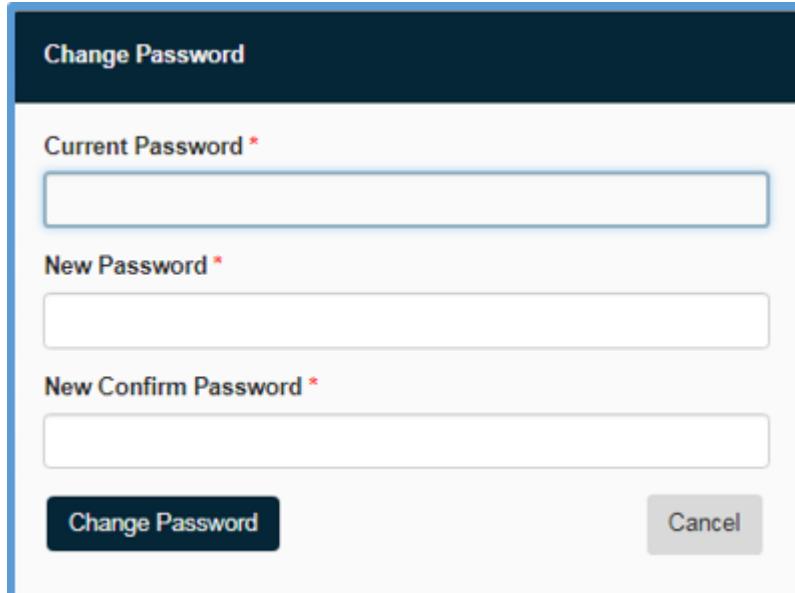
The User Profile dialogue will show your profile information. Use this dialogue to change first and last name or email. Select the "Save" button to keep changes or "Cancel" to exit the dialogue.

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

You can select the "Change Password" link to change your password.

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



The screenshot shows a modal dialogue box titled "Change Password". It contains three input fields: "Current Password *", "New Password *", and "New Confirm Password *". Below the fields are two buttons: "Change Password" (in a dark blue box) and "Cancel".

Figure: Change Password dialogue

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.

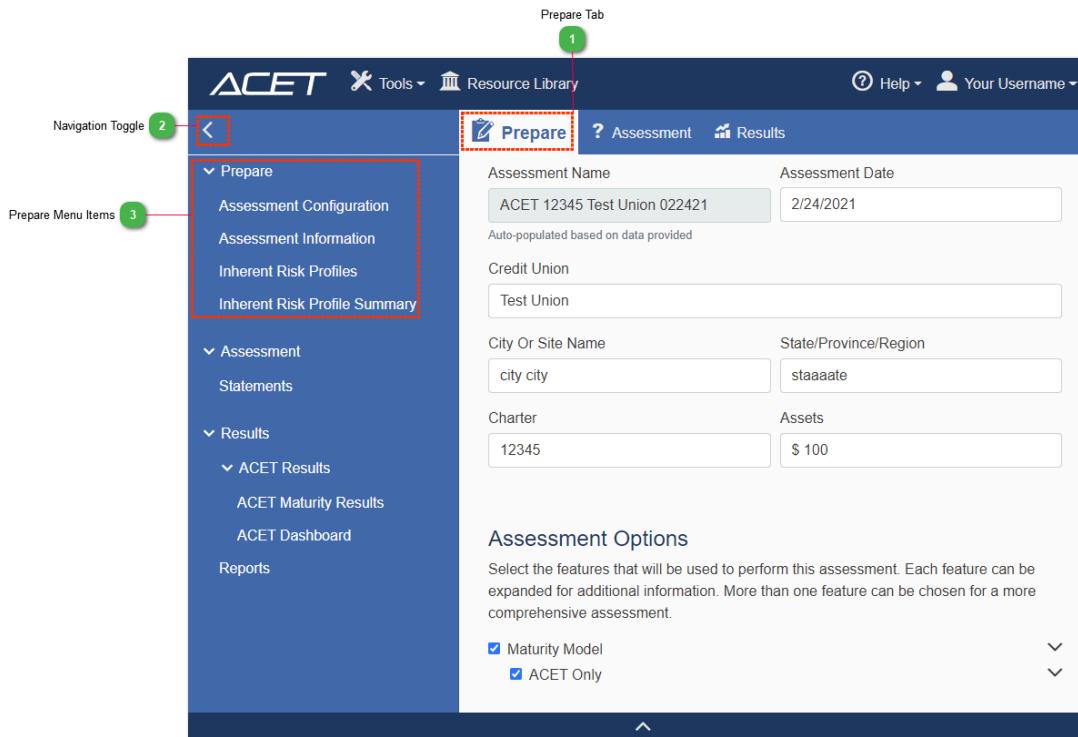


Figure: Prepare Button/Menu

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

- ▼ Prepare
 - Assessment Configuration
 - Assessment Information
 - Inherent Risk Profiles
 - Inherent Risk Profile Summary

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. See more in the [Assessment Information](#) section.

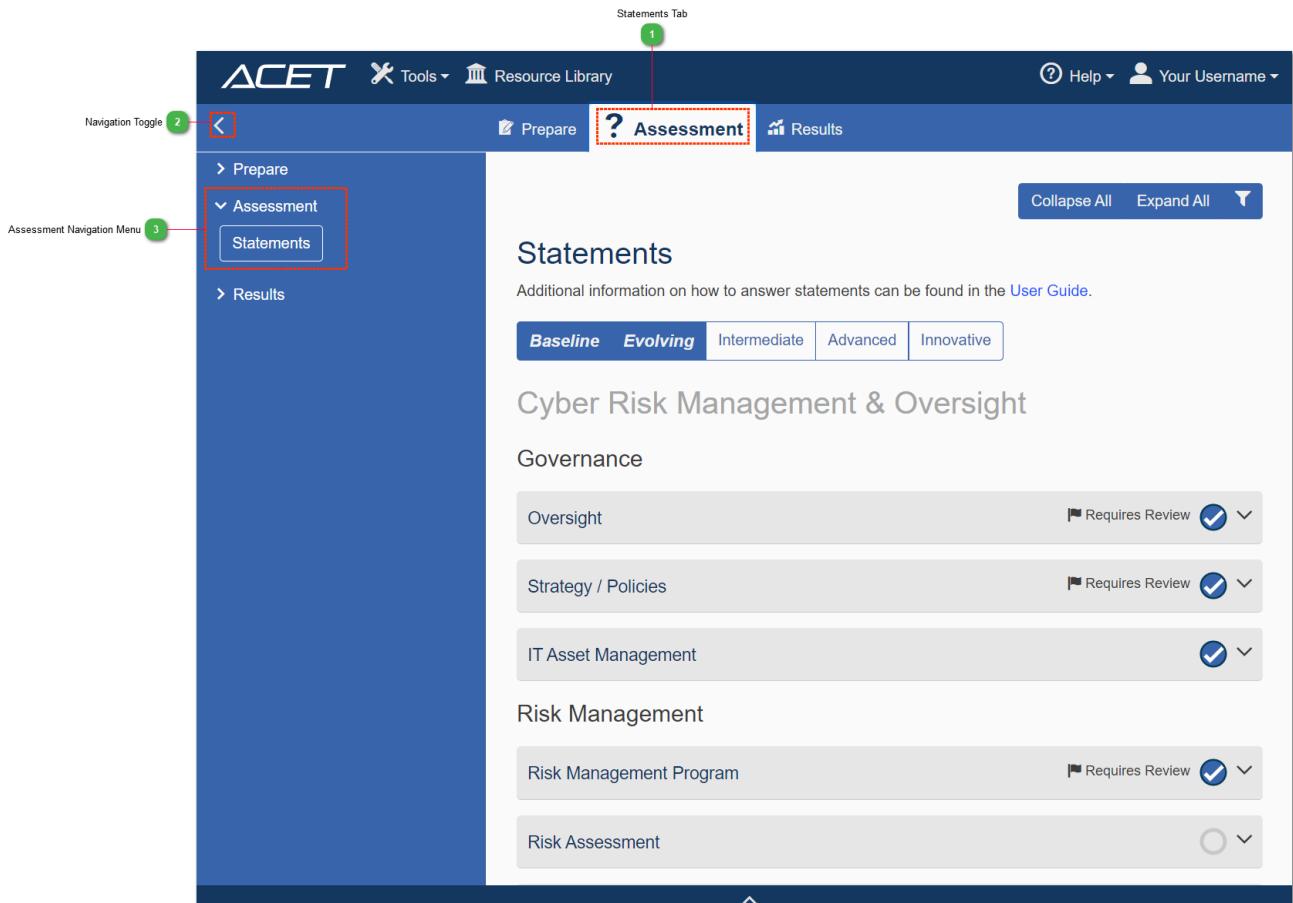


Figure: Assessment Button/Menu

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.

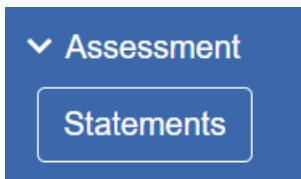
2 Navigation Toggle



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.

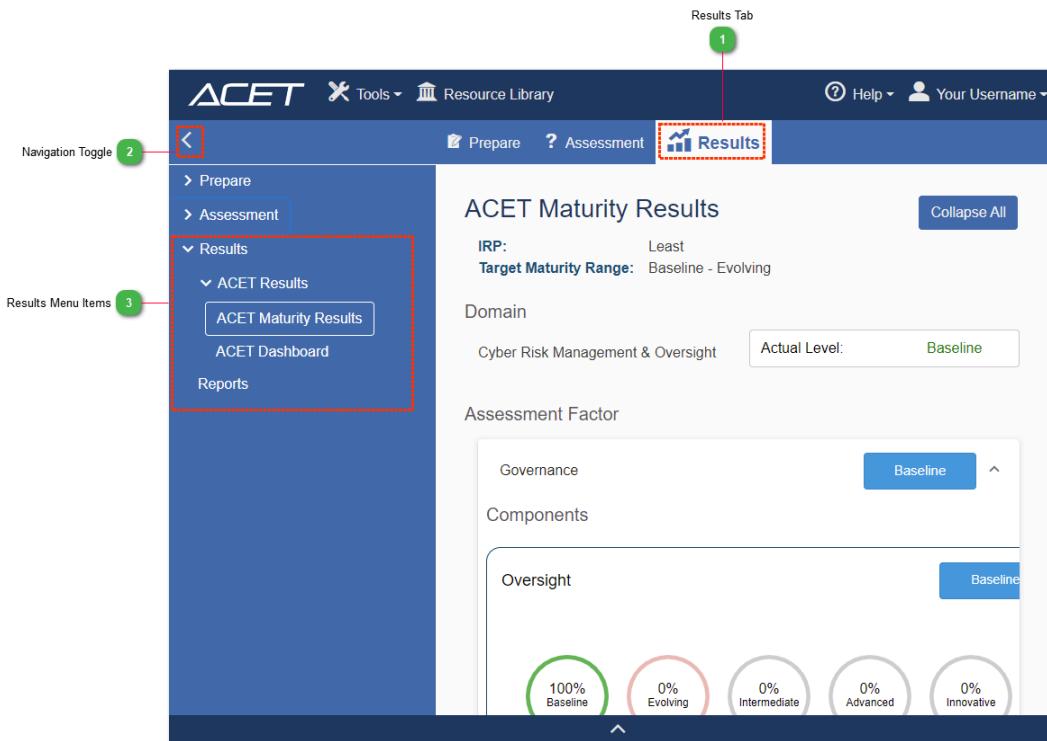


Figure: Results Button/Menu

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 you 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.

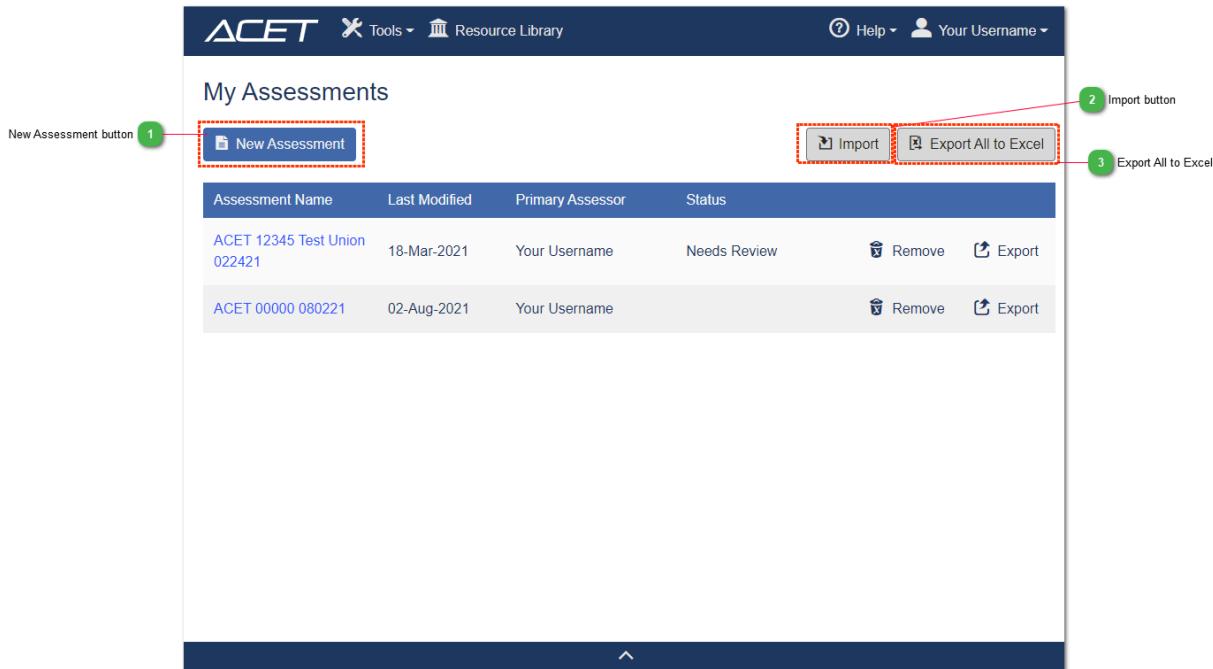


Figure: ACET Landing Page

1 New Assessment button



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

The first screen of the assessment preparation process is the [Assessment Configuration screen](#).

2 Import button



Select the Import button to import a .acet file. See [Importing a .acet file](#) for more information.

3 Export All to Excel



Each row represents an assessment so that all of your assessment data exists in a single sheet. Selecting "Export All 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 | 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 | |
| 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 | |

Figure: Export all ACET

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. This is also the screen where you will select your Assessment Options. 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.

The screenshot shows the ACET application interface. At the top, there is a navigation bar with the ACET logo, a Tools dropdown, a Resource Library link, a Help link, and a Your Username dropdown. Below the navigation bar, the main content area has a blue header bar with tabs: 'Prepare' (which is selected), 'Assessment', and 'Results'. The main content area is titled 'Assessment Configuration' and contains two main sections: 'Organization Details' and 'Assessment Options'.

Organization Details:

| | |
|---------------------------------------|-----------------|
| Assessment Name | Assessment Date |
| ACET 12345 Test Union 022421 | 2/24/2021 |
| Auto-populated based on data provided | |

Credit Union: Test Union

City Or Site Name: city city State/Province/Region: staaaate

Charter: 12345 Assets: \$ 100

Assessment Options:

Select the features that will be used to perform this assessment. Each feature can be expanded for additional information. More than one feature can be chosen for a more comprehensive assessment.

Maturity Model
 ACET Only

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 date picker enables you 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 you enter 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 you enter their charter number. Only numbers are accepted in this field.

Assets: The Assets box is where you enter 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 on the Maturity Model Selection page. It is preselected for ACET users. See the CSET guide (within the Help menu) for information regarding Standards and Network Diagrams.

Assessment Information

Contacts Management

Contacts Management is handled within the Assessment Information screen.

The screenshot shows a "Contacts" panel. At the top left is the title "Contacts". Below it is a section labeled "Your Username" with the value "Administrator". To the right of this section is the text "Assessment Owner". At the bottom left of the panel is a button labeled "+ Add Contact".

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.

The screenshot shows a "Add a New Contact" dialog box. At the top left is the label "Your Username" with the value "Administrator". To the right is the label "Assessment Owner". Below this are three input fields: "First Name" (with placeholder "First Name"), "Last Name" (with placeholder "Last Name"), and "Email" (with placeholder "Email Address"). Below these fields is a "Role" section with two buttons: "User" (which is selected) and "Administrator". At the bottom left is a blue "Save" button, and at the bottom right is a grey "Cancel" button.

Figure: Add a New Contact

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

The screenshot shows a 'Contacts' page with a header 'Your Username' containing 'Administrator' and a sub-header 'Assessment Owner'. Below this, there is a contact entry for 'Test User' with the email 'user@testing.com'. To the right of the contact entry are three icons: a pencil for 'Change', an envelope for 'Email', and a trash can for 'Remove'. At the bottom left is a button '+ Add Contact'.

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.

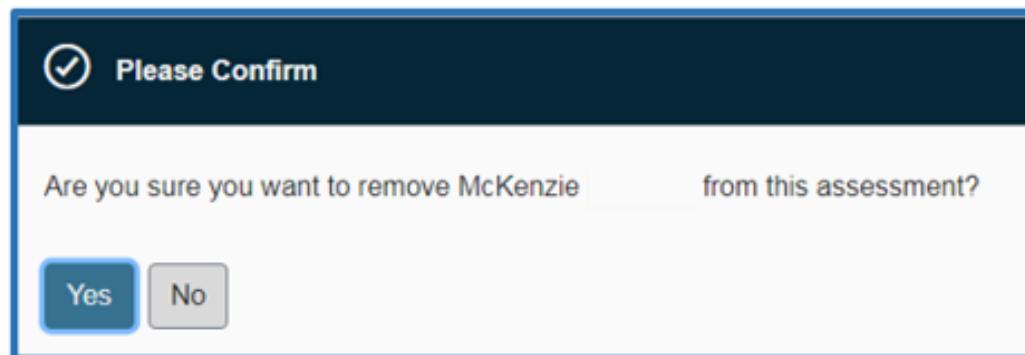


Figure. Contact Deletion dialogue

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

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. 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.

Review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain 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.

Inherent Risk Profiles

The IRP has [five risk areas](#) across five categories. It is measured on a scale from least risk to most risk in this order below:

IRP Categories 1

Technologies and Connection Types

IRP Questions 2

1. Total number of Internet service provider (ISP) connections (including branch connections)

Risk Levels

| | |
|---|--|
| 1 | No connections |
| 2 | Minimal complexity (1–20 connections) |
| 3 | Moderate complexity (21–100 connections) |
| 4 | Significant complexity (101–200 connections) |
| 5 | Substantial complexity (>200 connections) |

Risk Levels 3

IRP Icons 4

An Internet service provider (ISP) is a company (e.g., AT&T, Verizon, and CenturyLink) that provides its customers with Internet access. The total should include all external connections to the Internet, including from branches.

1 IRP Categories

Technologies and Connection Types

The IRP Categories break the IRP questions into groups.

2 IRP Questions

1. Total number of Internet service provider (ISP) connections (including branch connections)

Users select Risk Levels for each individual IRP Question.

3 Risk Levels

Risk Levels

- | | |
|---|--|
| 1 | No connections |
| 2 | Minimal complexity (1–20 connections) |
| 3 | Moderate complexity (21–100 connections) |
| 4 | Significant complexity (101–200 connections) |
| 5 | Substantial complexity (>200 connections) |

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.

4 IRP Icons



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

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

 Comments : The comments box allows you to leave a comment about the particular IRP question.

Inherent Risk Profile Summary

The Inherent Risk Summary page displays the Inherent Risk levels for the questions you answered on the [Inherent Risk Profiles](#) page.

The screenshot shows the ACET platform interface. At the top, there's a dark header bar with the ACET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' button, and a 'Your Username' dropdown. Below the header is a blue navigation bar with tabs: 'Prepare' (which is selected), 'Assessment', and 'Results'. The main content area is titled 'Inherent Risk Profile Summary'. It features a table with categories on the left and risk levels (1-5) on the right. The table data is as follows:

| Category | Inherent Risk | | | | |
|--|---------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Technologies and Connection Types | 0 | 0 | 1 | 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 | 1 | 0 | 0 |

Below the table, it says 'Overall Risk Level is 3 - Moderate'. There's a dropdown labeled 'Override Risk Level' set to 'No Override'. At the bottom, there are 'Back' and 'Next' buttons.

Figure: Inherent Risk Profile Summary

You 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. You are encouraged to provide a reason for IRP override.

Assessment Section

The assessment section is where you answer ACET statements. 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.

The screenshot shows the ACET Assessment screen. At the top, there is a navigation bar with the ACET logo, 'Tools' dropdown, 'Resource Library' link, 'Help' dropdown, and 'Your Username' link. Below the navigation bar, there are three tabs: 'Prepare' (selected), 'Assessment' (highlighted in blue), and 'Results'. On the right side of the header, there are 'Collapse All' and 'Expand All' buttons. The main content area is titled 'Statements' and contains the following elements:

- Cybersecurity Maturity Level filter (1):** A horizontal button with five options: Baseline (selected), Evolving, Intermediate, Advanced, and Innovative. The 'Evolving' option is highlighted with a red dotted border.
- Domain header (2):** A box labeled 'Cyber Risk Management & Oversight' with a red dotted border.
- Component header (3):** A box labeled 'Governance'.
- Assessment Factor header (4):** A box labeled 'Oversight'.
- Question/Requirement text (5):** A detailed statement for Stmt 1: 'Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.' Below the statement are five icons: a speech bubble, a person icon, a speech bubble with a red dot, a document icon, and a lightbulb icon. To the right of the statement are four buttons: 'Yes' (green), 'No' (red), 'NA' (blue), and 'Yes(C)' (yellow). A small checkmark icon is also present. Below the statement is a 'Reviewed' button.
- Statement 2:** 'Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.' Icons and buttons are similar to Stmt 1.
- Statement 3:** 'Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.' Icons and buttons are similar to Stmt 1.

Figure: Assessment Screen

1

Cybersecurity Maturity Level filter

| | | | | |
|-----------------|-----------------|--------------|----------|------------|
| Baseline | Evolving | Intermediate | Advanced | Innovative |
|-----------------|-----------------|--------------|----------|------------|

The filter shows in italics the levels that you have been assigned and displays statements in those levels below. You 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.

The blue highlighted levels are within your minimum target.

Bold and italicised levels are within your range.

To learn more, see the [ACET Maturity Results](#) section.

2

Domain header

Cyber Risk Management & Oversight

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

3

Component header

Governance

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

4

Assessment Factor header

Oversight

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

5

Question/Requirement text

Stmt 1 Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.
Baseline

The Statement text contains the exact ACET statements.

Statement Details, Resources, and Comments

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

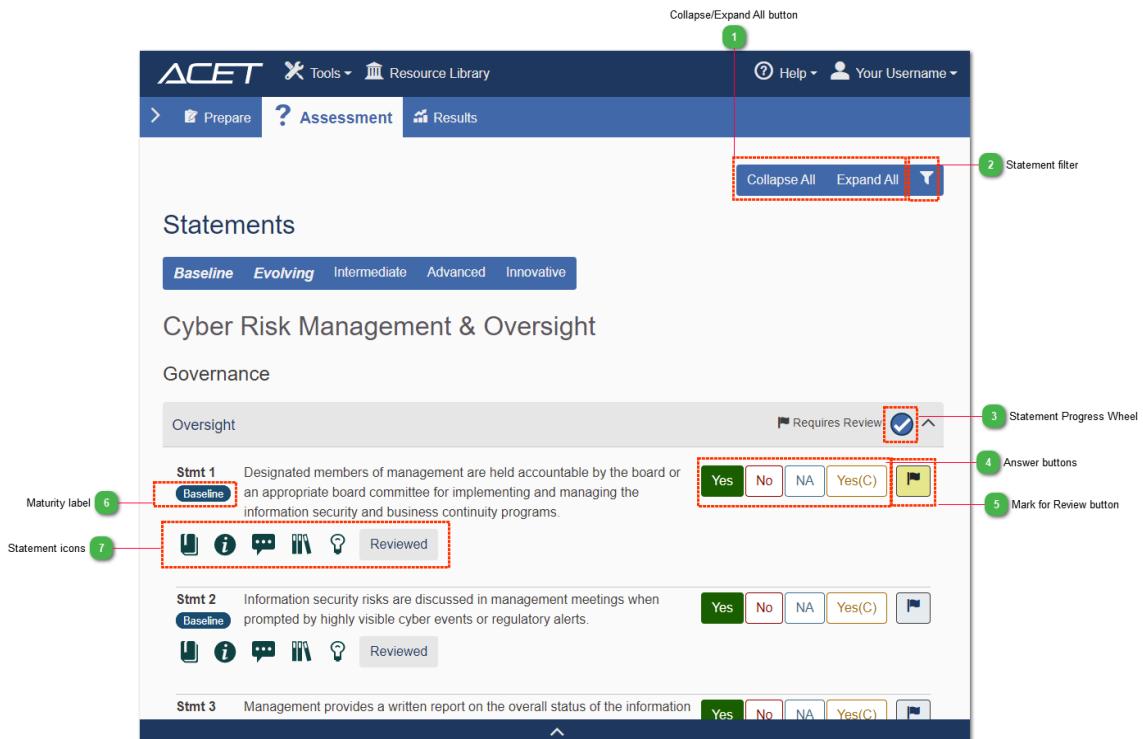


Figure: Statement Details, Resources, and Comments Screen

1 Collapse/Expand All button

Collapse All Expand All

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 you 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 you have 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 you to mark a statement for future review.

6 Maturity label

Baseline

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

7

Statement icons



Reviewed

The Statement icons are described in detail below.

Exam Step button : The Exam Step button will show or hide detailed ways to verify responses to the statement.

See the [Exam Step 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 you 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 you 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 you to create an observation record to associate with the statement.

See the [Observations Section](#) for more information.

Reviewed

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

Exam Step

The Exam Step section gives additional details into how to ensure that the statement is being met.

| | | | | | | |
|----------------------------------|---|------------|-----------|-----------|---------------|--|
| Stmt 1 Baseline | Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. | Yes | No | NA | Yes(C) | |
| | Reviewed | | | | | |
| | Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine compliance with Gramm Leach Bliley Act (GLBA) and other regulatory guidance. | | | | | |
| | Review the Board Package (or delegated board committee report) and Meeting Minutes, the IT Steering Committee Meeting Minutes or other oversight committee meeting minutes that have a responsibility for the Information Security and Business Continuity Programs for discussion and approval of the Information security and business continuity programs. | | | | | |
| | Discuss with management the information security roles and responsibilities and internal reporting structure to verify appropriate information security and business continuity planning reporting channels exists for staff, management, and the board. | | | | | |

Figure: Exam Step

Supplemental Section

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

Stmt 1 Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.

Baseline Yes No NA Yes(C)

Reviewed

The board or a board committee should be tasked for the oversight of these programs and should ensure compliance with the requirements of the programs by the financial institution's management, employees, and contractors. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to ensure appropriate compliance with the financial institution's policies, standards, and procedures.

Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine compliance with Gramm Leach Bliley Act (GLBA) and other regulatory guidance. Review the Board Package (or delegated board committee report) and Meeting Minutes, the IT Steering Committee Meeting Minutes or other oversight committee meeting minutes that have a responsibility for the Information Security and Business Continuity Programs for discussion and approval of the Information security and business continuity programs. Discuss with management the information security roles and responsibilities and internal reporting structure to verify appropriate information security and business continuity planning reporting channels exists for staff, management, and the board.

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 you to add comments to any assessment statement during the assessment process. The figure below describes the comment process.

The screenshot shows a statement from the ACET assessment screen. The statement is titled "Stmt 1 Baseline" and contains the text: "Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs." Below the statement are several icons: a document, an information sign, a speech bubble with a red dot (indicating comments), a bar chart, and a lightbulb. To the right of these icons is the word "Reviewed". At the top right of the statement area are four buttons: "Yes" (green), "No" (red), "NA" (light blue), and "Yes(C)" (orange). To the far right is a small flag icon. Below the statement is a text input field with the placeholder text "Need more information on this.".

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 you to easily see what statements have comments when scrolling through the list of questions.

The Comments text box allows you 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 sources and Help documentation as seen in the figure below.

Stmt 1 Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.

Baseline

Yes No NA Yes(C)

 Reviewed

| Source Documents | Section |
|--|-------------------|
| FFIEC Cybersecurity Assessment Tool | D1.G.Ov.B |
| Help Documents | Section |
| Cybersecurity Framework V 1.1 | ID.GV-4 |
| Cybersecurity Framework V 1.1 | ID.RM-1 |
| IT Examination Handbook for Information Security | IS.I:pg3 |
| IT Examination Handbook for Information Security | IS.I:pg4: |
| IT Examination Handbook for Information Security | IS.WP.2.3: |
| IT Examination Handbook for Management | MGT.III.C.3:pg28: |
| IT Examination Handbook for Management | MGT.WP.2.2.g: |
| IT Examination Handbook for Management | MGT.WP.2: |

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.

The screenshot shows the 'Observations Section' for Stmt 1. The statement text is: 'Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.' Below the text are several status buttons: 'Yes' (green), 'No' (red), 'NA' (light blue), 'Yes(C)' (orange), and a flag icon. Underneath the buttons are icons for document, info, message, and lightbulb, followed by the word 'Reviewed'. At the bottom is a blue 'Add an Observation' button.

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 : 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 you to enter information about a statement that has a "no" answer. Any statement that has been answered "No" could potentially have an 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.

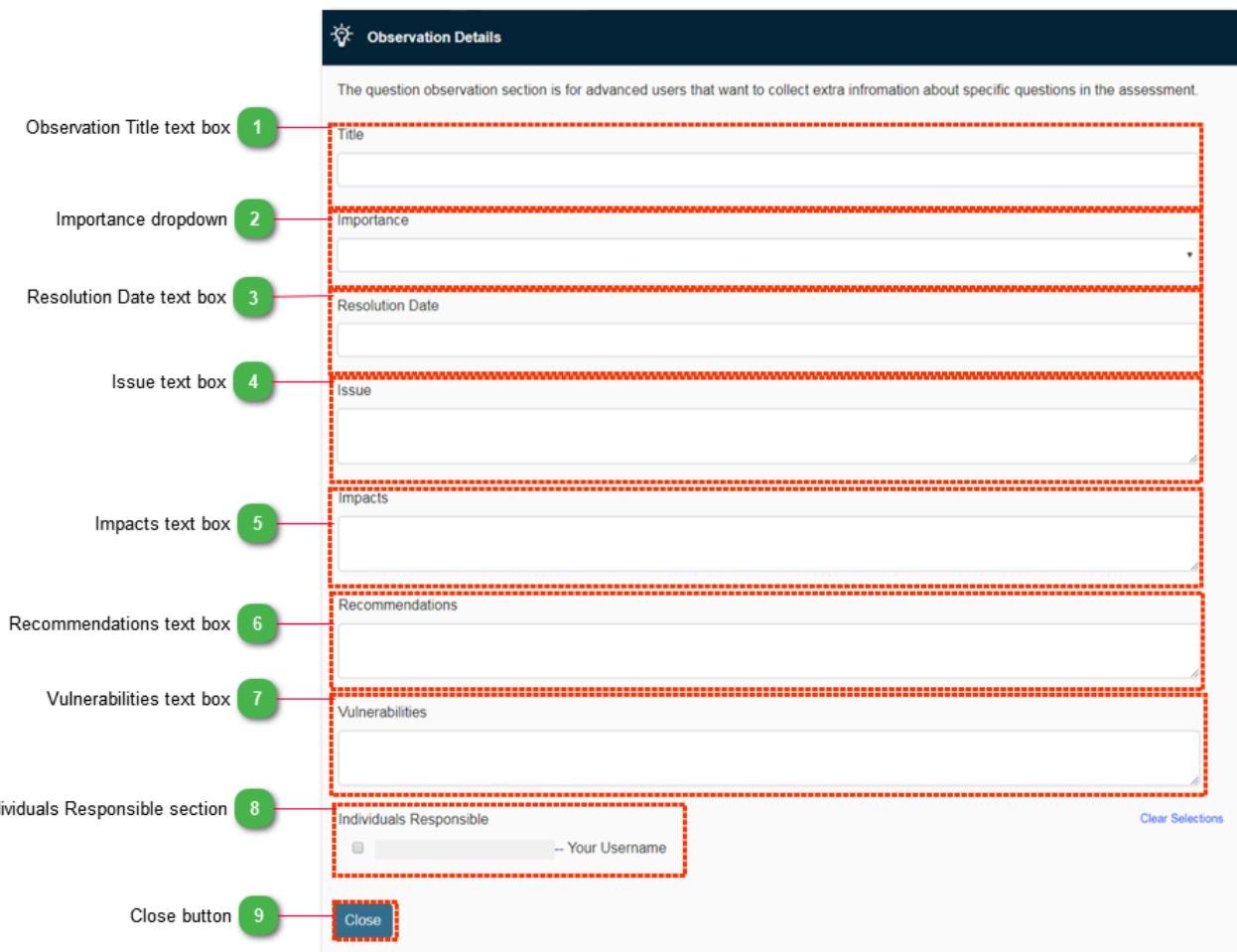


Figure: Observation Details Window

1 Observation Title text box

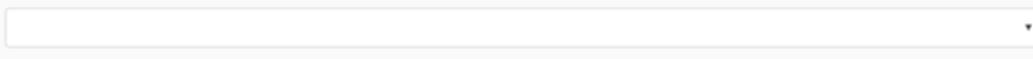
A zoomed-in view of the 'Title' text input field. The field is labeled 'Title' and contains a placeholder text '... Your Username'. To the left of the input field is a green circle containing the number 1, indicating it corresponds to the 'Observation Title text box' described in the figure caption.

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

2

Importance dropdown

Importance



A dropdown menu with three options: "Low", "Medium", and "High".

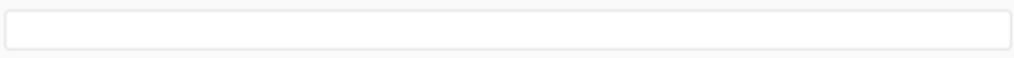
The Importance dropdown allows you to assign an importance level to the observation record.

Valid values are Low, Medium, and High.

3

Resolution Date text box

Resolution Date



An input field for entering a date.

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

4

Issue text box

Issue



An input field for defining a detailed explanation of the issue or problem related to why the statement was answered "No".

5

Impacts text box

Impacts



An input field for defining potential or real impacts that the issue may or is currently having on systems, assets, and/or procedures.

6

Recommendations text box

Recommendations



An input field for providing recommendations or steps for resolving the issues or problems defined in the observation.

7

Vulnerabilities text box

Vulnerabilities



An input field for listing vulnerabilities.

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

8

Individuals Responsible section



The Individuals Responsible section allows you to assign individuals to be responsible for fixing the issues identified in the observation record. The Contacts checklist 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. Add a contact in the contact window below, if the individual responsible isn't in the current list.

9

Close button

A screenshot of a user interface showing a "Close" button located in the bottom-left corner of a window.

The Close button will close the Observations Details window.

Statements Filter

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

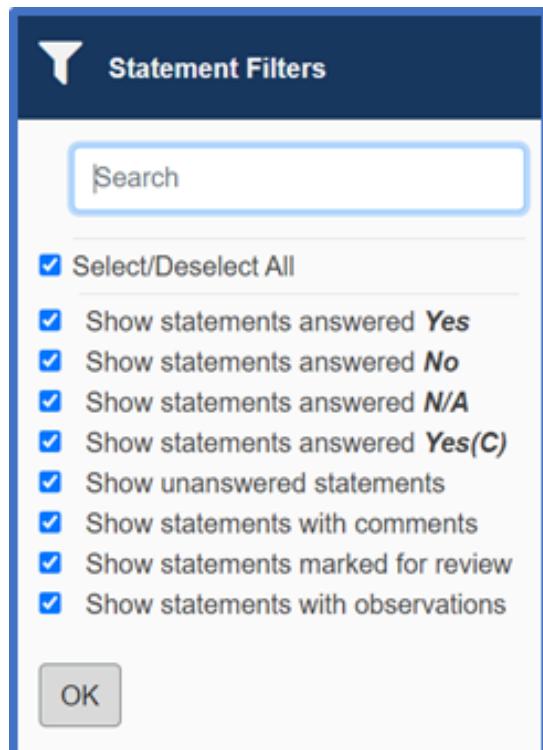


Figure: Statement Filter

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.

The screenshot shows the ACET (Assessment) interface. At the top, there's a dark header bar with the ACET logo, a 'Tools' dropdown, a 'Resource Library' link, and a 'Help' and 'Your Username' dropdown. Below the header is a blue navigation bar with tabs: 'Prepare' (selected), 'Assessment' (selected), and 'Results'. On the right side of the main content area, there are 'Collapse All', 'Expand All', and a search icon.

Statements

Additional information on how to answer statements can be found in the [User Guide](#).

Showing Only Filtered Questions

Baseline **Evolving** Intermediate Advanced Innovative

Cyber Risk Management & Oversight

Baseline **Evolving** Intermediate Advanced Innovative

Threat Intelligence & Collaboration

Baseline **Evolving** Intermediate Advanced Innovative

Cybersecurity Controls

Figure: No results visible error message

Results Section

Once you've completed answering statements, 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 your level based on statements answered during the assessment process.

The Results sections consist of ACET Maturity Results, Dashboard, and Reports. This section will describe each area.

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.

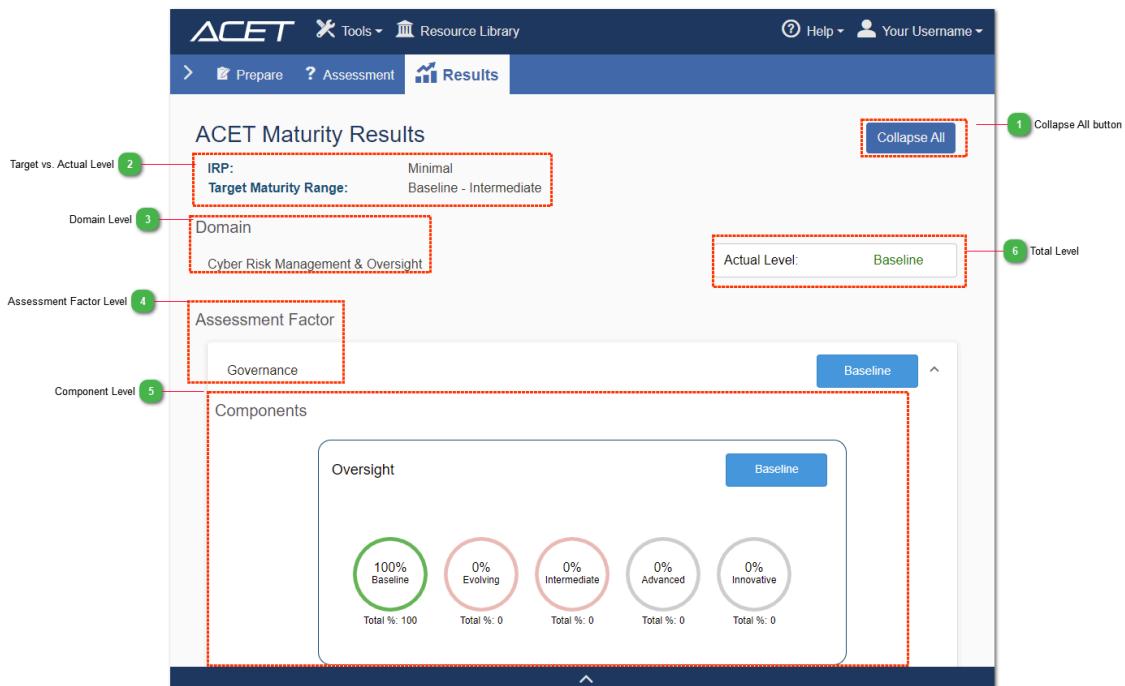


Figure: Cybersecurity Maturity screen

1 Collapse All button

Collapse All

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 Target vs. Actual Level

| | |
|------------------------|-------------------------|
| IRP: | Minimal |
| Target Maturity Range: | Baseline - Intermediate |

The IRP level shows the level assigned after filling out the information on the [Inherent Risk Profiles](#) screen.

The Target Maturity Range shows your expected range based on IRP and maturity.

3 Domain Level

Domain

Cyber Risk Management & Oversight

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.

4 Assessment Factor Level

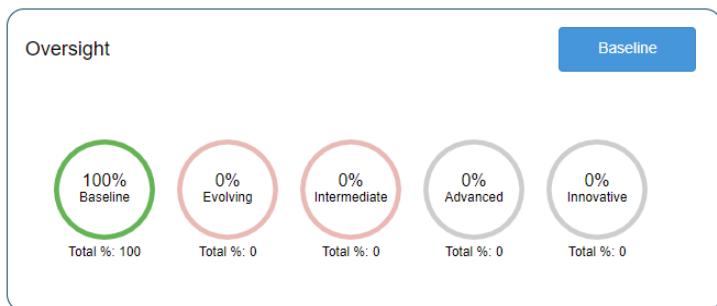
Assessment Factor

Governance

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

5 Component Level

Components



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.

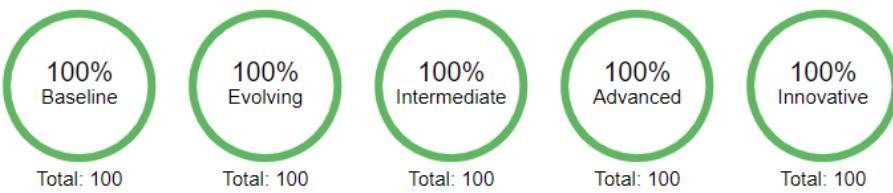
The colors for the components level is defined below:

Gray= Isn't necessary for a 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 you 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.

6

Total Level

Actual Level: **Baseline**

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

Ad Hoc

If it is red and says "Ad Hoc" then the statements have been fully answered but do 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.

The screenshot shows the ACET Dashboard interface. At the top, there are navigation tabs: 'Prepare' (highlighted), 'Assessment', and 'Results'. The main content area is titled 'ACET Dashboard'.

- Prepare section (1):** Contains demographic information:
 - Credit Union Name: Test Union
 - Charter: 14598
 - Assets: \$100,000
- Inherent Risk Profile section (2):** Contains a table of inherent risk levels across various categories. The table has columns for Category and Inherent Risk (1-5).

| Category | Inherent Risk | | | | |
|--|---------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Technologies and Connection Types | 1 | 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 | 1 | 0 | 0 | 0 | 0 |

Overall Risk Level is **1 - Least**
Override Risk Level is **2 - Minimal**
Override Reason:
- Cybersecurity Maturity section (3):** Contains a table of cybersecurity maturity levels across domains. Both domains are at 'Baseline' level.

| Domain | Maturity Level |
|---|----------------|
| Domain 1: Cyber Risk Management & Oversight | Baseline |
| Domain 2: Threat Intelligence & Collaboration | Baseline |

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: | 14598 |
| 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

| Category | Inherent Risk | | | | |
|--|---------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Technologies and Connection Types | 1 | 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 | 1 | 0 | 0 | 0 | 0 |

Overall Risk Level is **1 - Least**
Override Risk Level is **2 - Minimal**
Override Reason:

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: Cyber Risk Management & Oversight | Baseline |
| Domain 2: Threat Intelligence & Collaboration | Baseline |

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 you 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 hard copy of the results to be used in meetings, for management communications, and as a way to assign tasks to technical staff. Combined with the online analysis, these reports can help to clearly understand where weaknesses are and where improvements should be made.

This section will describe how to use the Reports Screen.

Report Screen

The Report screen is shown in the figure below.

The screenshot shows the ACET application interface. At the top, there is a dark blue header bar with the ACET logo on the left, followed by navigation links: Tools, Resource Library, Help, and Your Username. Below the header, there is a horizontal menu bar with three items: Prepare, Assessment, and Results. The 'Results' item is highlighted with a blue background and white text. The main content area is titled 'Reports' and contains a section for 'ACET Reports'. This section lists several report types: ACET Executive Summary, ACET Gap Report, ACET Comments and Marked for Review, ACET Answered Statements, and ACET Compensating Controls. Each item is a blue link. At the bottom left of the content area, there is a blue 'Back' button. The overall layout is clean and professional, typical of a web-based assessment tool.

Figure: Report screen

To generate a report click on the specific report link on the Report 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](#).

NOTE: Some reports aren't available if you haven't completed your assessment. Completion is answering all statements within your target level. The image below shows what the Report screen looks like if you haven't completed your assessment.

The screenshot shows the ACET application interface. At the top, there is a dark blue header bar with the ACET logo, a 'Tools' dropdown, a 'Resource Library' link, a 'Help' link, and a 'Your Username' dropdown. Below the header is a blue navigation bar with four tabs: 'Prepare', 'Assessment', 'Results' (which is selected), and 'Reports'. The main content area has a light gray background. A section titled 'Reports' contains a heading 'ACET Reports'. Below this, a yellow rectangular box contains a warning message: '⚠ Some reports are disabled until all statements have been answered.' To the left of the warning message is a small exclamation mark icon. Underneath the warning, there is a list of report names: 'ACET Executive Summary', 'ACET Gap Report', 'ACET Comments and Marked for Review', 'ACET Answered Statements' (which is bolded), and 'ACET Compensating Controls'. At the bottom left of the content area is a blue 'Back' button.

Figure: Disabled Reports

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.

Gap

This gap report lists the statements that are "No" answers.

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.

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, a 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.

Gaps: The Gaps 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 comments 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 range, your answers, and whether there is a comment attached to the statement.

The statement set is determined by your maturity range.

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 |
| FFIEC | Federal Financial Institutions Examination Council |
| FFIEC CAT | FFIEC Cybersecurity Assessment Tool |
| ICS | Industrial Control System |
| IIS | Internet Information Services |
| IRP | Inherent Risk Profile |
| IT | Information Technology |
| JSON | JavaScript Object Notation |
| NA | Not Applicable |
| NCUA | National Credit Union Administration |
| PDF | Portable Document Format |
| SAL | Security Assurance Level |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| XML | eXtensible Markup Language |

Key Terms

| Term | Explanation |
|----------------------|---|
| Ad Hoc | Statements are answered but don't meet the baseline level |
| Advanced | Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. The majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned. |
| Assessment Factor | The ACET assessment Components break down further into Assessment Factors. |
| Assessment Report | A summary report of results for each question including user responses, statement of actual requirements (or deficiencies), answers concerning the overall SAL, and associated help documents. |
| Baseline | Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance. |
| Component | The ACET assessment Domains break down further into Components. |
| Component Diagram or | A network topology that best represents the industrial control system configuration. The 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 |

| | |
|--------------------------|---|
| Network Diagram | 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. |
| Domain | The ACET assessment breaks down into 5 domains: Cyber Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, and Cyber Incident Management and Resilience. This is the highest level of breakdown within the assessment. |
| Evolving | Evolving maturity is characterized by the additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond the protection of customer information to incorporate information assets and systems. |
| Exam Step | Exam steps are suggested ways for verifying responses. |
| Incomplete | A section is incomplete if all statements have not been answered. |
| Innovative | Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses. |
| Intermediate | Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies. |
| Observations | Observations are a way to add a "finding" or "discovery" to a statement. It allows you to document the issue, priority, when it occurred, and assign responsibility. |
| Security Assurance Level | <p>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.</p> <p>The SAL ranges from Low to Very High.</p> |
| Security Categories | <p>The security categories are related to the NIST 800-53 Standards and are defined as:</p> <p>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.</p> <p>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.</p> <p>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.</p> |

| | |
|-------------------------|--|
| Security Categorization | <p>The NIST 800-53-related security categorizations of Low, Moderate, and High are explained as:</p> <p>LOW:</p> <p>The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p>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.</p> <p>MODERATE:</p> <p>The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p> <p>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.</p> <p>HIGH:</p> <p>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.</p> <p>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.</p> |
| Security Level | The rating of High, Moderate, or Low for Confidentiality, Integrity, and Availability according to FIPS 199 and NIST SP800-60. |
| Supplemental | Supplemental provides additional information to aid in answering statements. |
| Yes (C) | Yes Compensating. This is an answer option on the Statements screen. |

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 |
| 10.2 | March 2021 | 10.2 beta release. Includes updates to navigation with new feature selections, removal of CSET instructions, new and updated reports. |
| 10.2.1 | June 2021 | Minor changes to Disclaimer and UI |
| 11.0 | August 2021 | Full release version |