NCUA
National Credit Union Administration

The Automated Cybersecurity Evaluation Toolbox

User Manual

August 2025

[This page intentionally left blank]

Table of Contents

Introduction to the ACET

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

Introduction

The 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 is an assessment of a credit union's inherent risk and cybersecurity maturity. ACET provides a repeatable, measurable and transparent process for assessing the level of cyber preparedness across federally insured institutions.

The ACET consists of two parts: Inherent Risk Profile (IRP) and Cybersecurity Maturity. The IRP 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.

Objectives and Benefits

The ACET's primary objective is to reduce the risk of cyberattacks by identifying potential cybersecurity vulnerabilities within a system or an organization. It does this by implementing a simple, transparent process that can be used effectively by all critical infrastructure sectors to evaluate any network. Among other benefits, the ACET:

- 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.
- Helps identify 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 opportunities to discuss security practices within the user's facility.

Limitations of this Tool

The tool has a component focus rather than a system focus. Thus, 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, the ACET is only one component of a comprehensive control system security program. A security program based on an 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 fully and accurately answer all the questions provided by the ACET.

Disclaimer

The analysis, data, and reports in the 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.

The 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 the 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 the NCUA or the United States Government. Use of the NCUA seal without proper authorization violates federal law (for example, 18 U.S.C. §§ 506, 701, 1017) and is against NCUA policies governing usage of theseal.

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 or 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 from various operational areas in the organization. Organizations may add more team members as needed to address specific topics. Anyone in the organization who has had training or experience with the ACET should be included on the team.

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

Representatives from the areas below 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 or Topology (knowledge of IT infrastructure).
- IT Security or 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 or decision-maker).
- Industrial Control Systems (knowledge of industrial control system architecture and operations).
- System Configuration (knowledge of systems management).
- System Operations (knowledge of system operation).

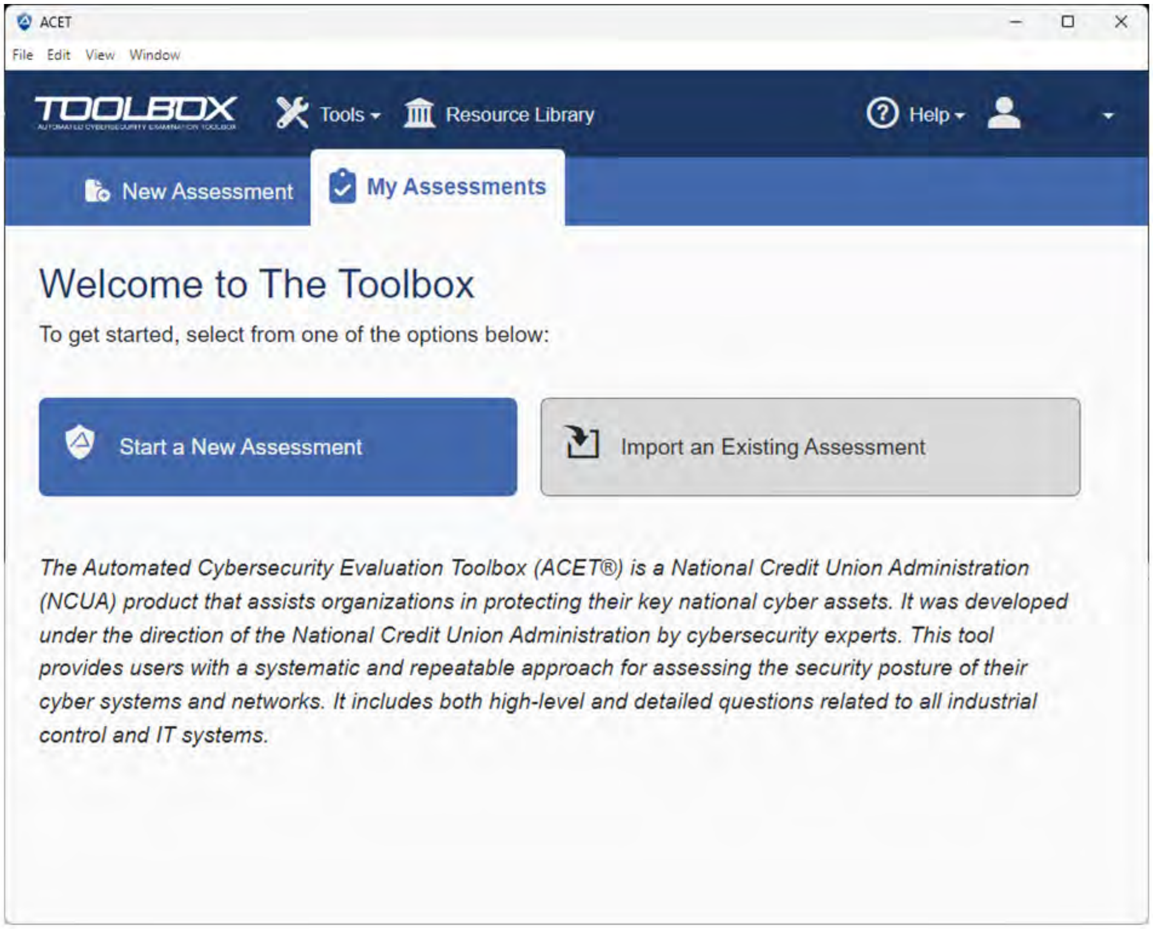
Getting Started

If you have not downloaded the ACET, follow the instructions noted in the ACET Quick Install Guide before proceeding. Once installed, you will see an ACET icon on your desktop.

Start the ACET by double clicking the ACET desktop icon.

The ACET will open to the My Assessments tab.

Figure: ACET My Assessments



Welcome to The Toolbox

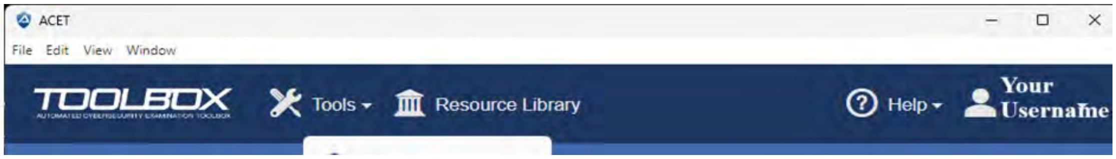
To get started, select from one of the options below:

The Automated Cybersecurity Evaluation Toolbox (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.

Title Bar

As shown in the figure below, the Title Bar allows the user to access high-level functions of the ACET.

Figure: Title Bar



Toolbox — The Toolbox Home button opens the user’s landing page.

Tools — The Tools button opens the Tools menu.

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

Help — The Help button opens the Help menu.

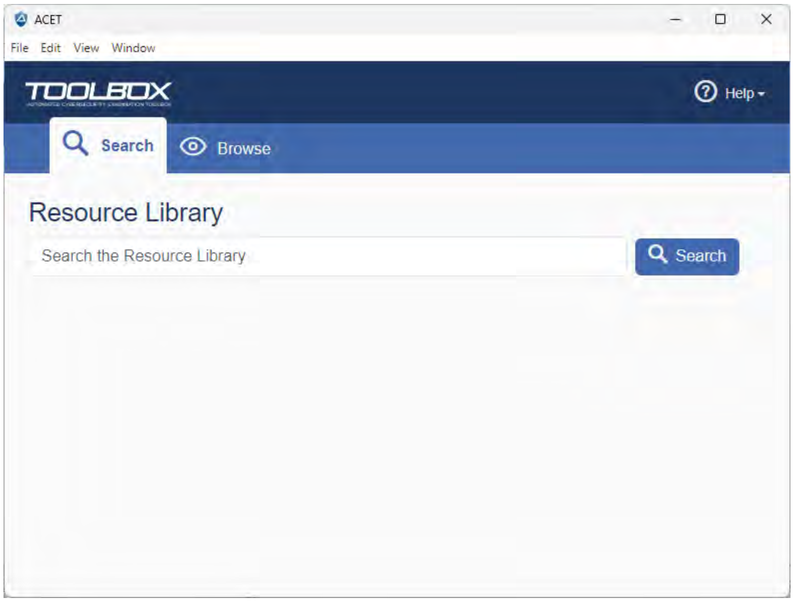
User Profile — This will display your username. The User Profile button opens the User Profile menu.

For more information on Resource Library and Help see the applicable sections for each within this guide.

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



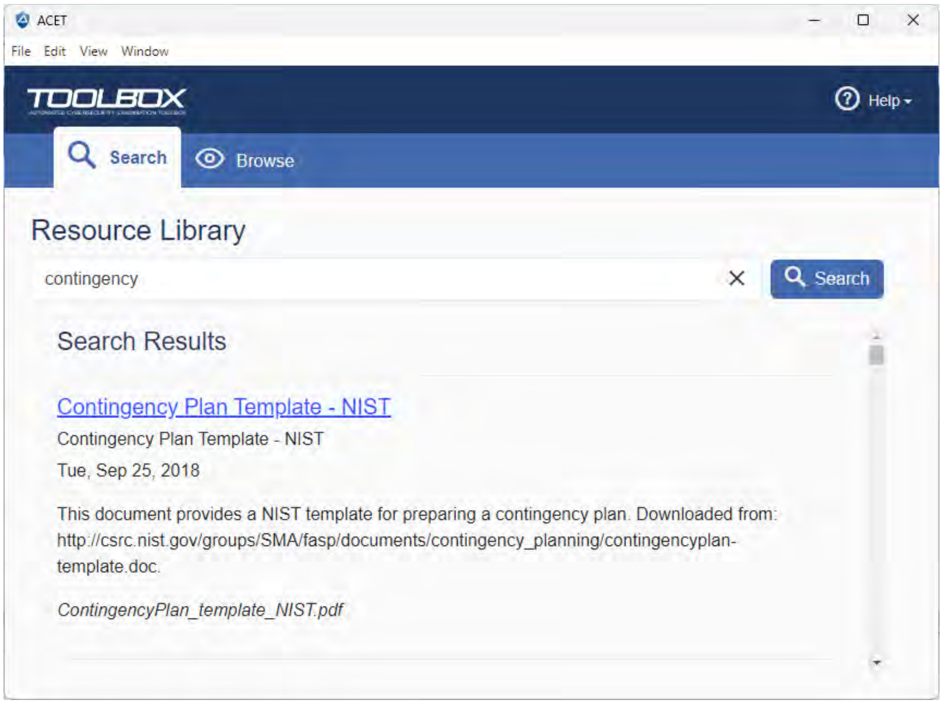
Search Screen

There are two ways 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, the ACET searches through all the documents for occurrences of the word "contingency," then ranks and presents them in an ordered list in the search results.

Figure: Resource Library Search screen



Resource Library

contingency

Search Results

Contingency Plan Template - NIST

Contingency Plan Template - NIST

Tue, Sep 25, 2018

This document provides a NIST template for preparing a contingency plan. Downloaded from: http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc.

ContingencyPlan_template_NIST.pdf

Search Tab — Clicking the search tab will display the search functions of the Resource Library. The Resource Library opens directly 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. These allow the user to expand the results by using symbols to represent unknown characters within a search term. 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 National Institute of Standards and Technology (NIST) Special Publication 800 series documents where the last two characters are substituted by the question mark wildcard character.

When the 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 "*Syber-Security*" will yield no results.

Topic Searches

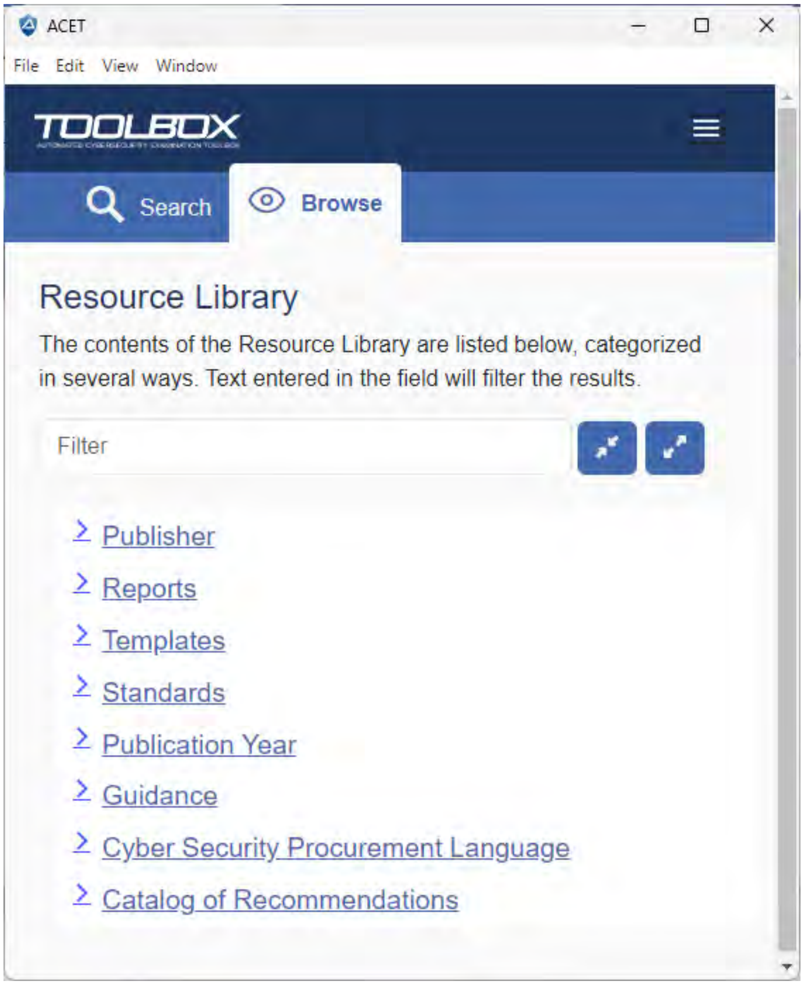
In most cases, the user will be searching for a specific subject; however,the search capability can also be used to search for types of documents. In the example above, the NIST SP800 document is a recommended practice. By entering "recommended practice" in the search text box, the user can return a list of all recommended practices developed by the Department of Homeland Security and other documents categorized also as a recommended practice.

Browse Screen

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

Figure: Resource Library document tree



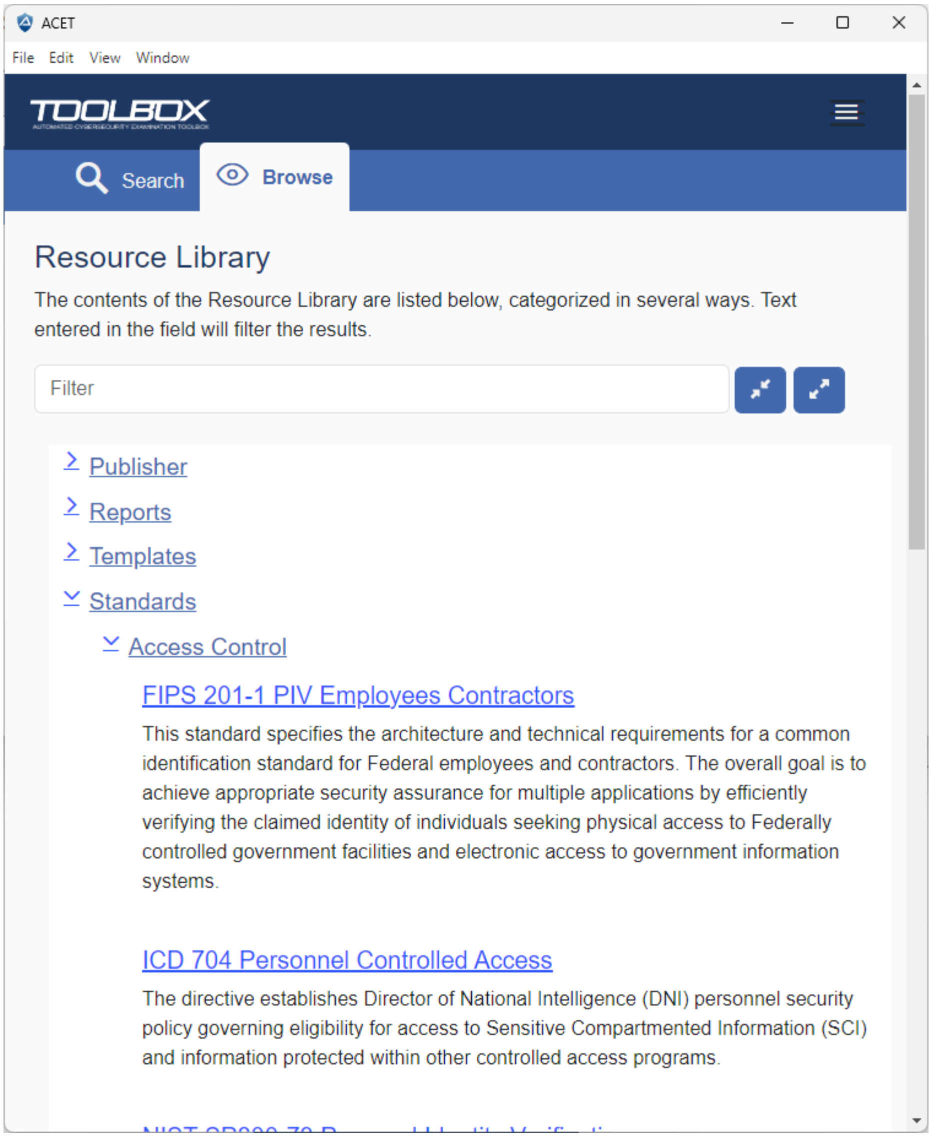
Resource Library

The contents of the Resource Library are listed below, categorized in several ways. Text entered in the field will filter the results.

- Publisher
- Reports
- Templates
- Standards
- Publication Year
- Guidance
- Cyber Security Procurement Language
- Catalog of Recommendations

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

Figure: Expanded document tree



Resource Library

The contents of the Resource Library are listed below, categorized in several ways. Text entered in the field will filter the results.

Filter

- Publisher
- Reports
- Templates
- Standards
  - Access Control

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.

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

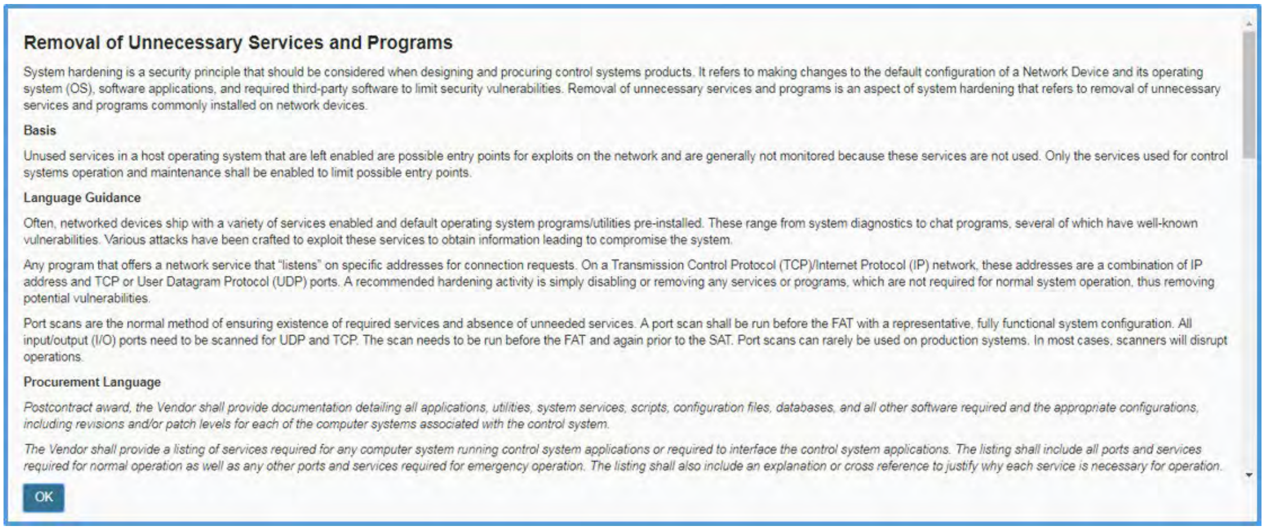
The options to browse by publisher and publication year are also available. They were added for those users looking for specific versions of documents or documents from a specific source. The documents listed under these headings are the same as in the rest of the tree but listed in a differing order.

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

Cyber Security Procurement Language

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

Figure: Cyber Security Procurement Language



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.

In this case, instead of a document being opened, the 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 Measures
- Site Acceptance Test Measures
- Maintenance Guidance

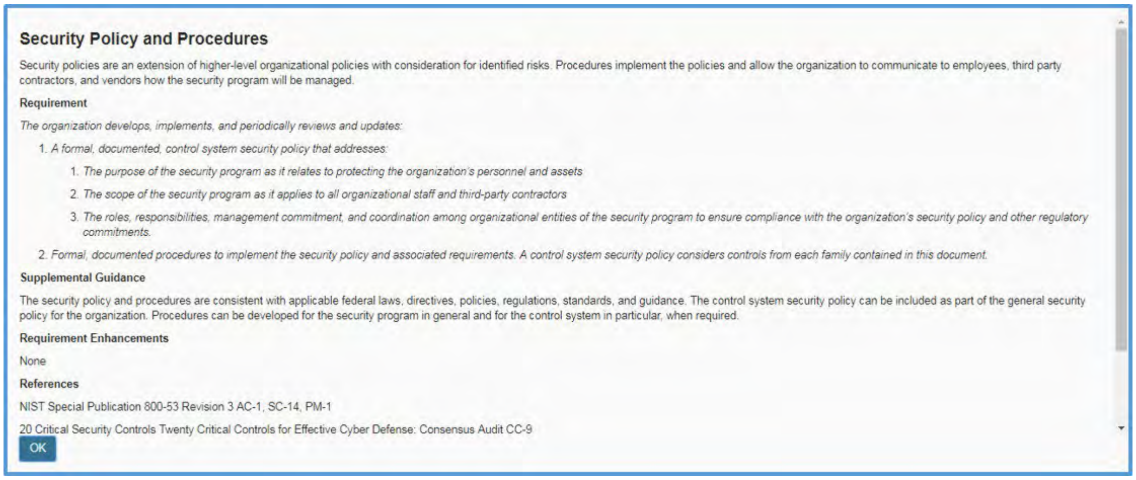
- Dependencies and
- References

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

Catalog of Recommendations

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

Figure: Catalog of Recommendations



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

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 ICS standards developers. Due to its popularity and comprehensive ICS requirements, it has become a principal standard in all versions of the ACET and in the ICS community at large besides 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, the ACET displays the catalog content. Each topic includes some or all the following sections:

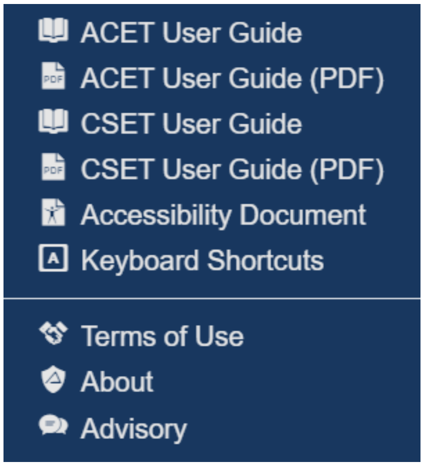
- Brief Overview of the Topic
- Requirement Text
- Supplemental Guidance
- Requirement Enhancements and
- References

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.

Figure: Help Menu



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

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

CSET User Guide — Clicking the Cyber Security Evaluation Tool (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 the ACET addresses accessibility issues including the use of high contrast mode and keyboard access.

See ACET Accessibility Features 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 ACET.

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 the ACET.

See Terms of Use for more information.

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

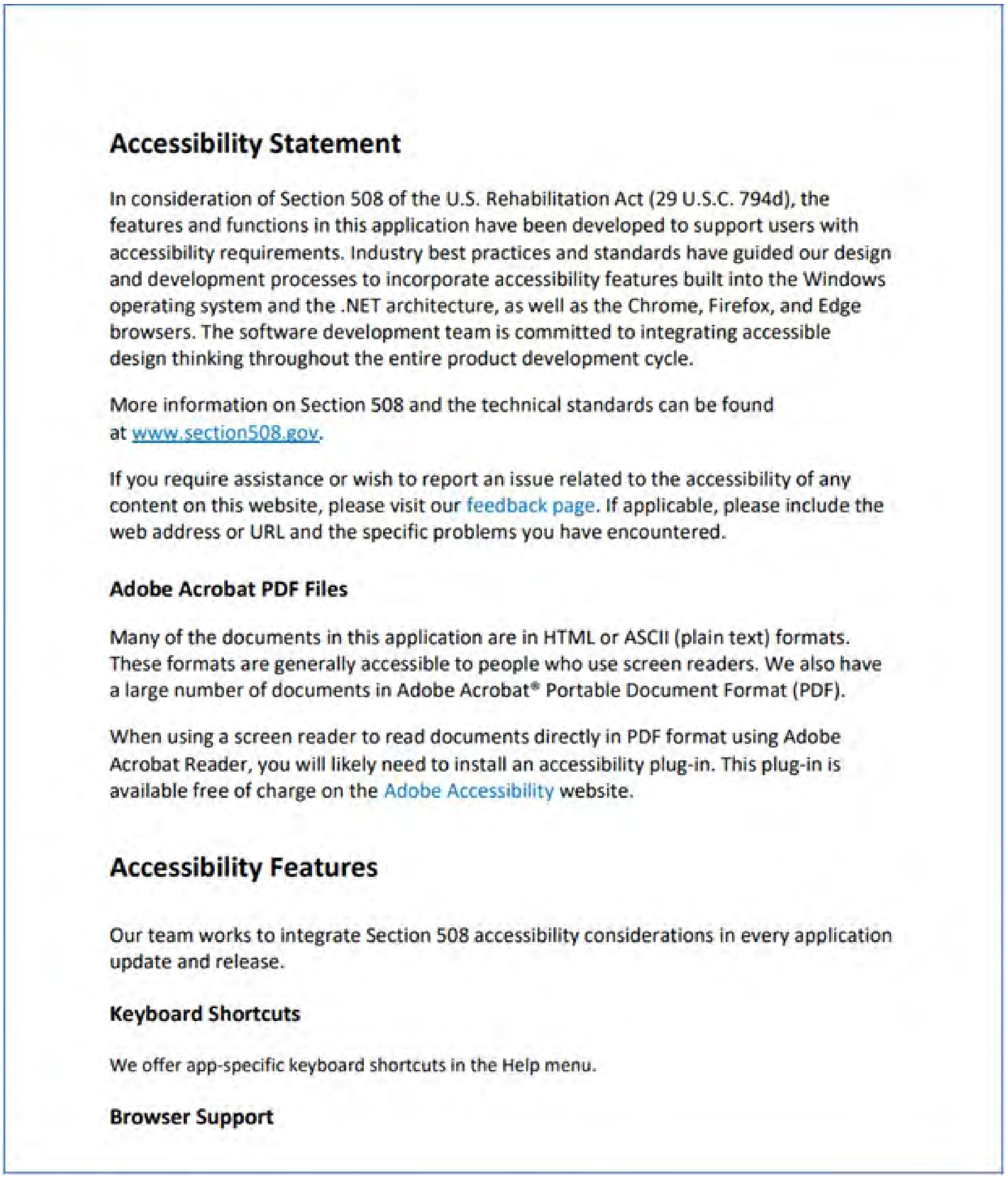
See About the ACET for more information.

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

ACET Accessibility Features

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

Figure: ACET Accessibility Features Document



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

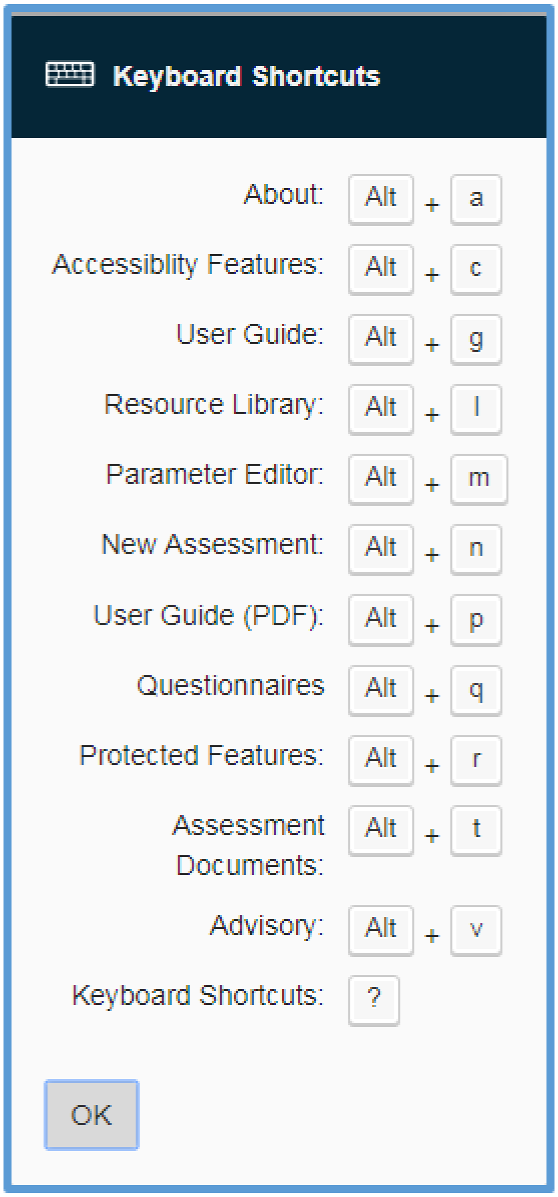
We offer app-specific keyboard shortcuts in the Help menu.

Browser Support

Keyboard Shortcuts

The figure below shows the ACET Keyboard Shortcuts document that can be accessed from the ACET's Help Menu.

Figure: ACET Keyboard Shortcuts Document



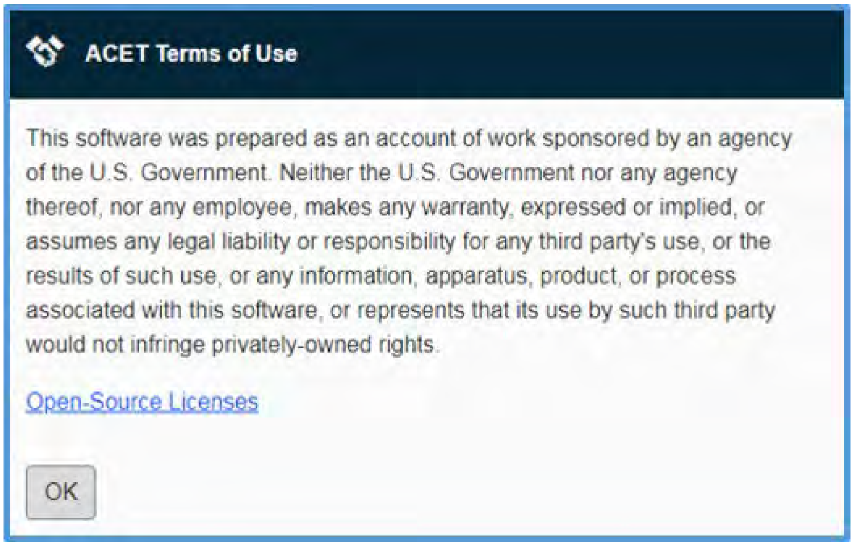
Keyboard Shortcuts

About:	Alt + a
Accessiblity Features:	Alt + c
User Guide:	Alt + g
Resource Library:	Alt + l
Parameter Editor:	Alt + m
New Assessment:	Alt + n
User Guide (PDF):	Alt + p
Questionnaires	Alt + q
Protected Features:	Alt + r
Assessment Documents:	Alt + t
Advisory:	Alt + v
Keyboard Shortcuts:	?

Terms of Use

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

Figure: Terms of Use



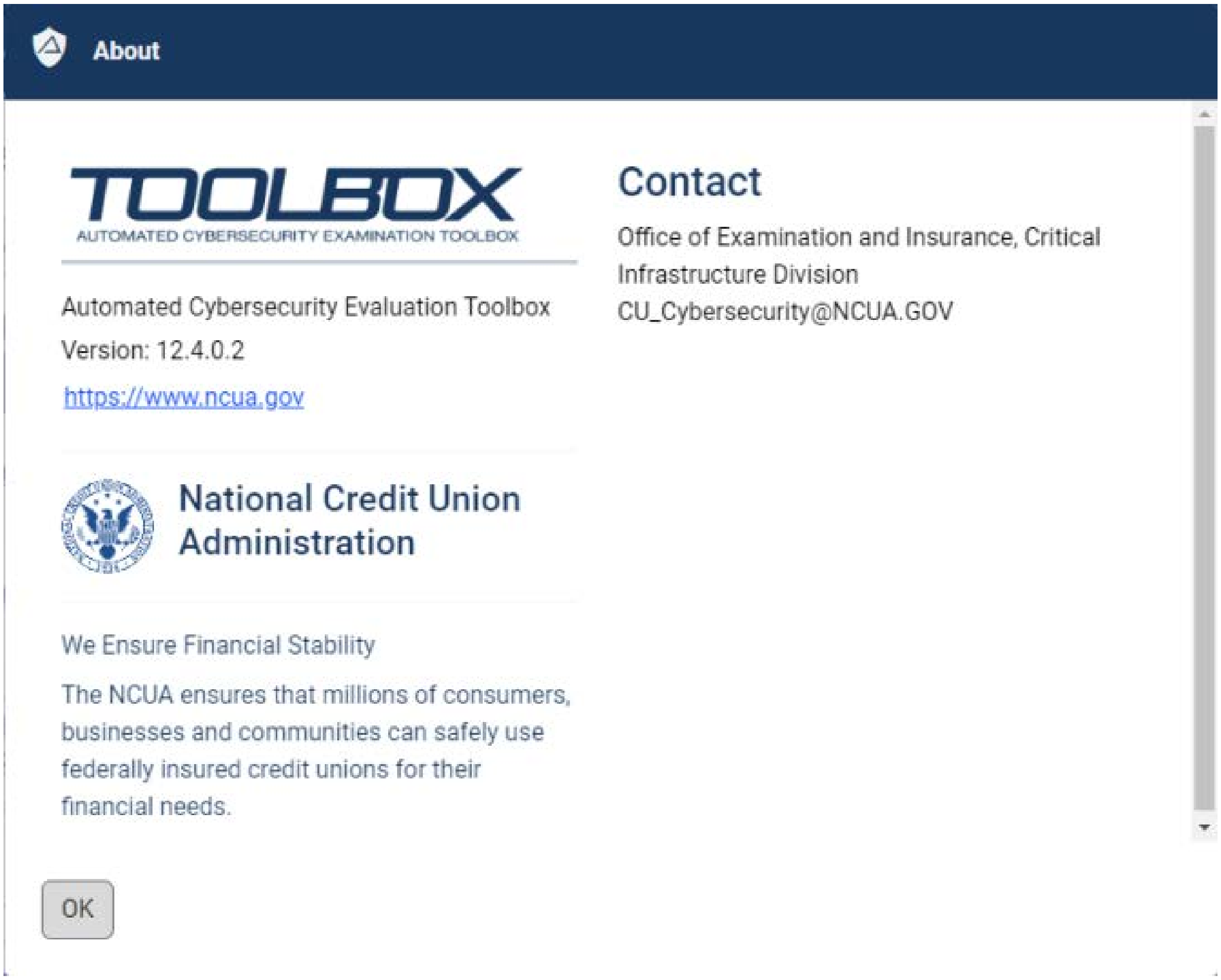
ACET Terms of Use

This software was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, or any information, apparatus, product, or process associated with this software, or represents that its use by such third party would not infringe privately-owned rights.

About the ACET

The About ACET window gives users more information about the ACET team. It includes contact information, a version number, and a link to the NCUA's website, which includes training information.

Figure: About ACET Window



Automated Cybersecurity Evaluation Toolbox

Version: 12.4.0.2

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.

Contact

Office of Examination and Insurance, Critical Infrastructure Division

CU_Cybersecurity@NCUA.GOV

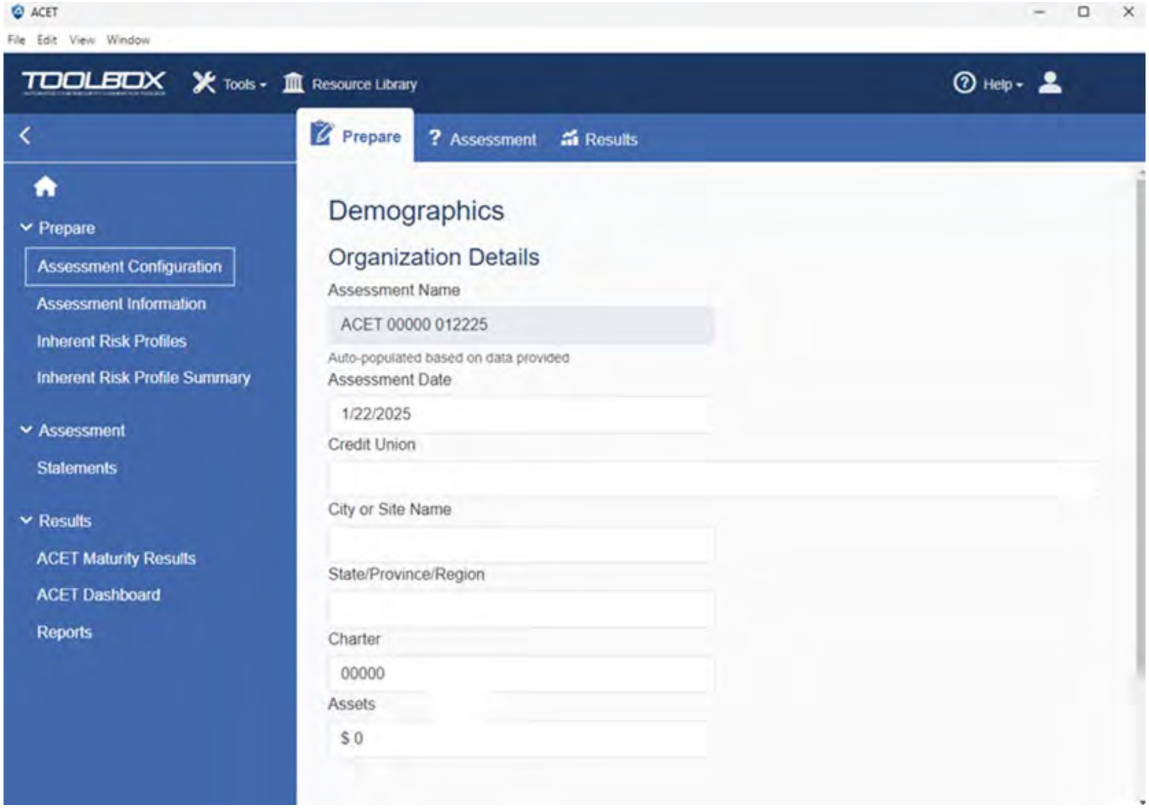
Operation Menus

This section addresses the ACET's main operation menus. 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 displays the buttons and menu.

Figure: Prepare Button or Menu



Demographics

Organization Details

Assessment Name: ACET 00000 012225

Auto-populated based on data provided

Assessment Date: 1/22/2025

Credit Union:

City or Site Name:

State/Province/Region:

Charter: 00000

Assets: $ 0

Prepare Tab — Clicking the Prepare button will display the Assessment Configuration screen.

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

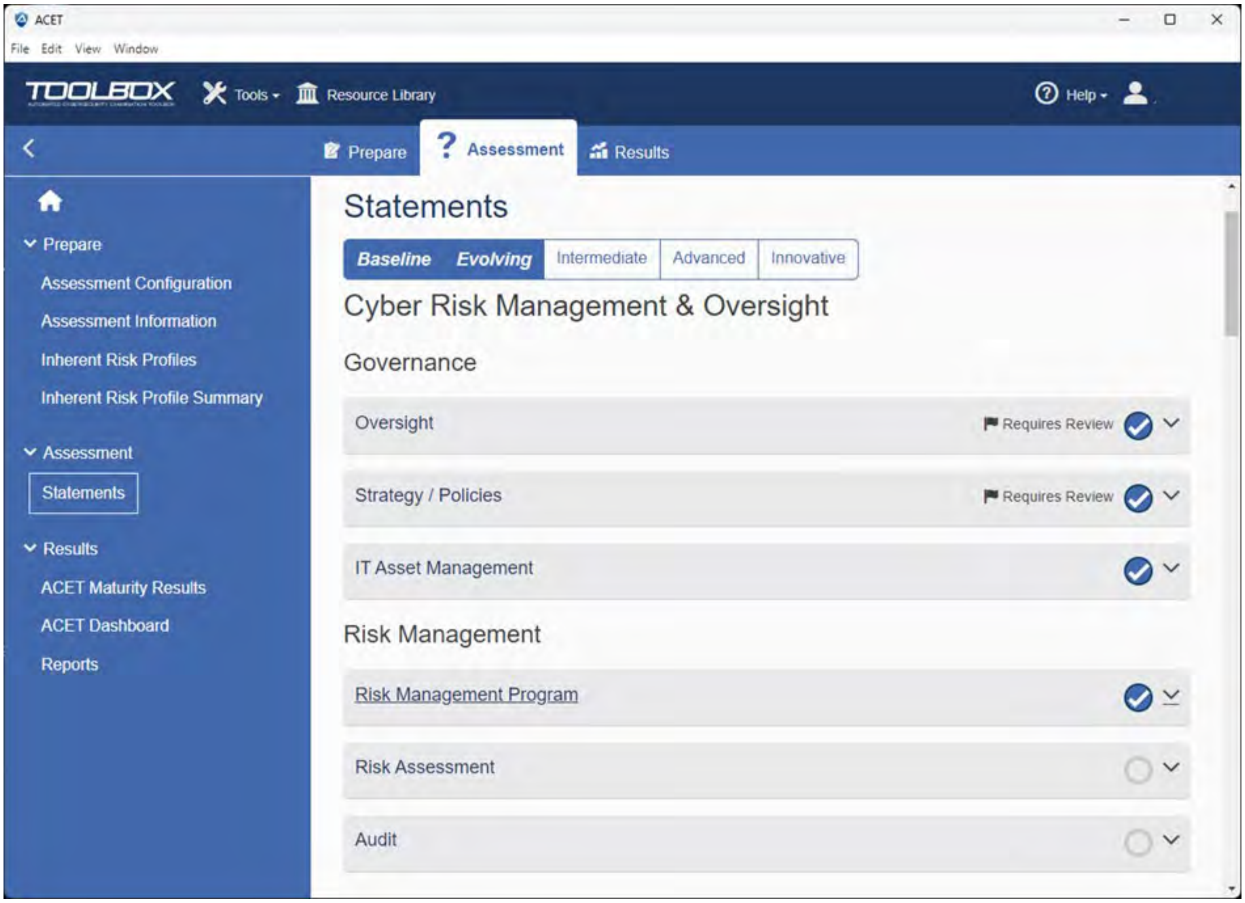
Prepare Menu Items — The Prepare menu items indicate the screens encountered by the user during the preparation process.

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

Assessment Menu

The Assessment menu allows quick access to the assessment statements and categories. The figure below shows the Assessment menu navigation. See more in the Assessment Information section.

Figure: Assessment Button/Menu



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

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

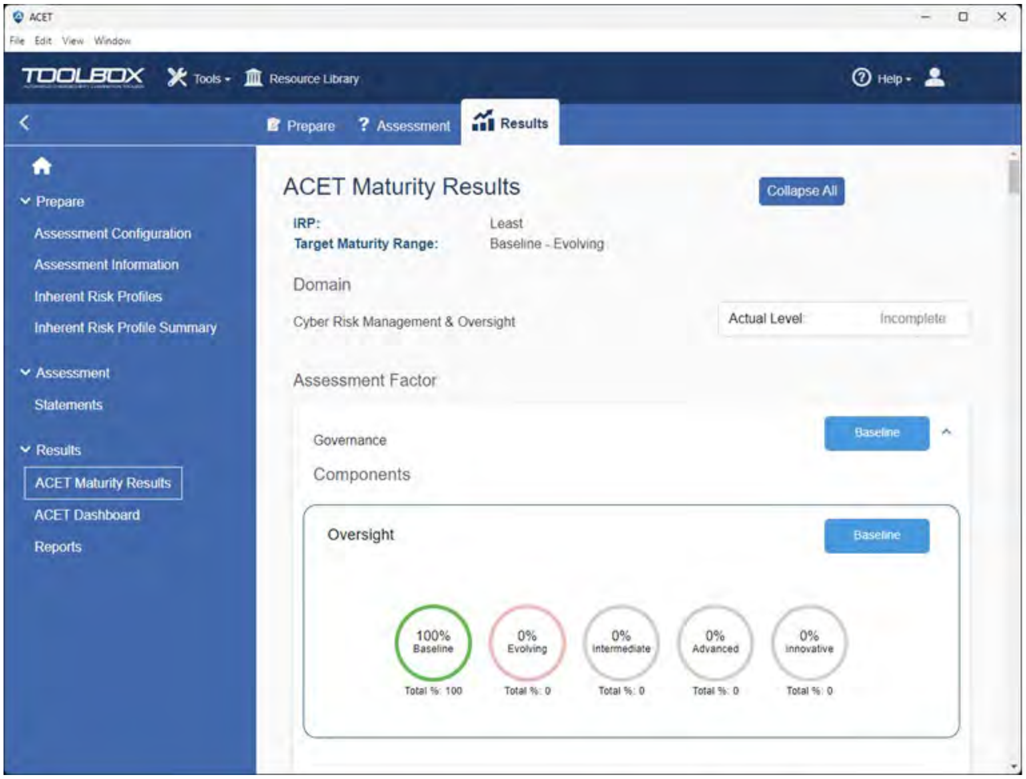
Navigation Toggle — Use the Navigation Toggle to open and close the Navigation Menu. This is located on the left side of the screen.

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



ACET Maturity Results

IRP: Least
Target Maturity Range: Baseline - Evolving

Domain

Cyber Risk Management & Oversight — Actual Level: Incomplete

Assessment Factor

Governance — Baseline

Components

Oversight — Baseline

100% Baseline	0% Evolving	0% Intermediate	0% Advanced	0% Innovative
Total %: 100	Total %: 0	Total %: 0	Total %: 0	Total %: 0

Results Tab — Clicking the Results button will display the Results Overview screen.

Navigation Toggle — Use the Navigation Toggle to open and close the Navigation Menu. This is located on the screen's left side.

Results Menu Items — The Results menu items indicate the screens available to the user in the main Results Section. These are ACET Maturity Results, ACET Dashboard, and Reports.

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.

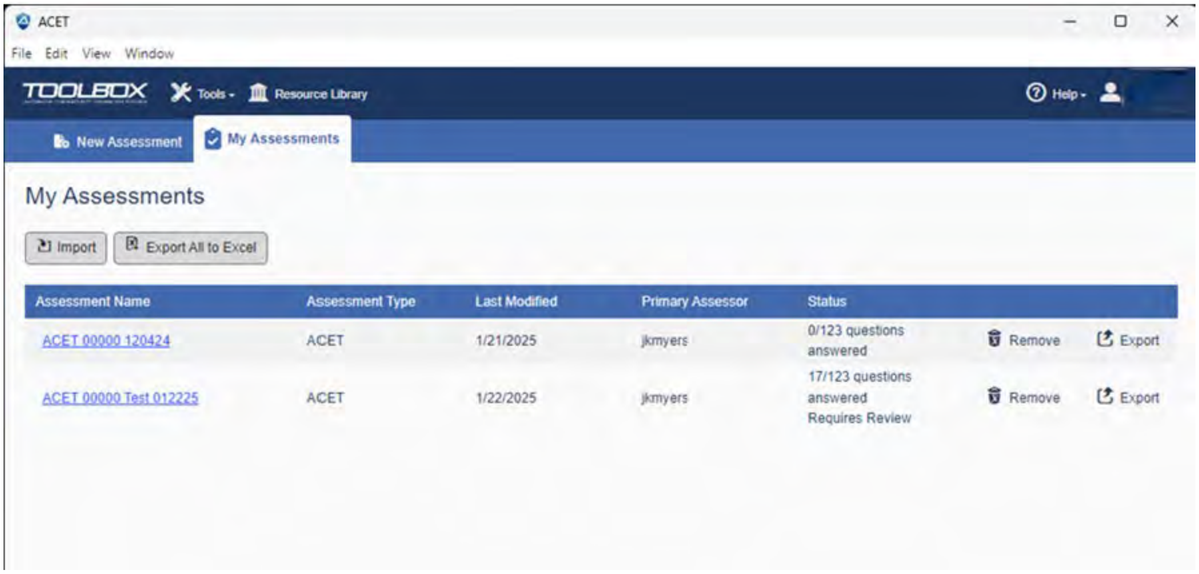
Prepare Section

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

The 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



Assessment Name	Assessment Type	Last Modified	Primary Assessor	Status		
ACET 00000 120424	ACET	1/21/2025	jkmyers	0/123 questions answered	Remove	Export
ACET 00000 Test 012225	ACET	1/22/2025	jkmyers	17/123 questions answered Requires Review	Remove	Export

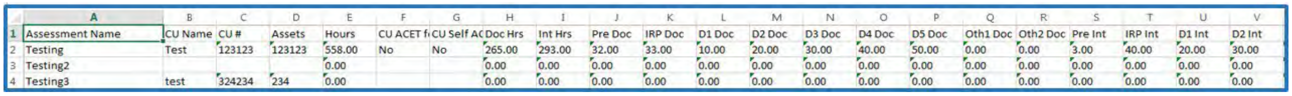
New Assessment — Clicking the New Assessment button will start the assessment preparation process that will allow you to address important areas before answering questions.

Import — Select the Import button to import a .acet file.

See Importing a .acet file for more information.

Export All to Excel — Each row represents an assessment so that all your assessment data exists in a single sheet as shown below. Selecting this button downloads all ACET assessments from the My Assessments screen.

Figure: Export all ACET



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

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

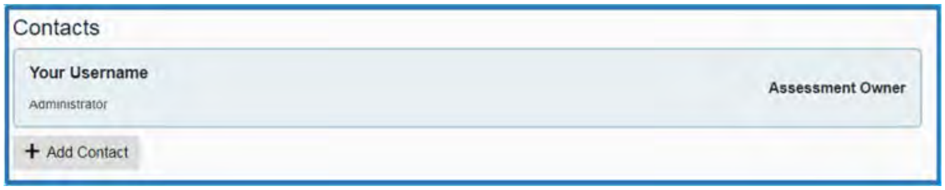
See Exporting an ACET Assessment for more information.

Assessment Information

Contacts Management

Contacts Management is handled within the Assessment Information screen.

Figure: Contacts Management Panel



Contacts

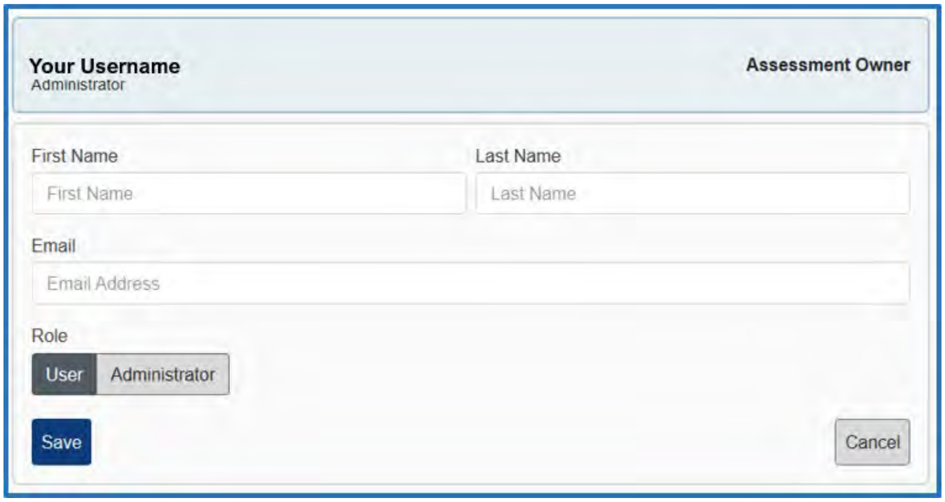
Your Username
Administrator

Assessment Owner

The Contacts panel shows the Assessment Owner's name (the user who created the assessment) followed by their email address.

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

Figure: Add a New Contact



Your Username
Administrator

Assessment Owner

First Name: First Name

Last Name: Last Name

Email: Email Address

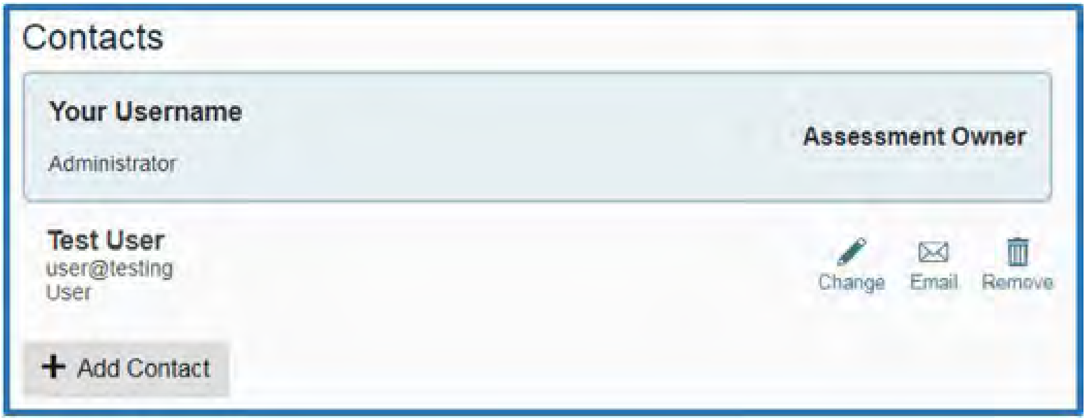
Role: User | Administrator

Add a New Contact — After selecting "Add Contact," a dialogue box will open. 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 Administrators can add and remove contacts to an assessment and delete assessments. There must be an Administrator assigned to an assessment.

Select Save or Cancel to exit the dialogue.

Figure: Added user to assessment and contact icons


Contacts

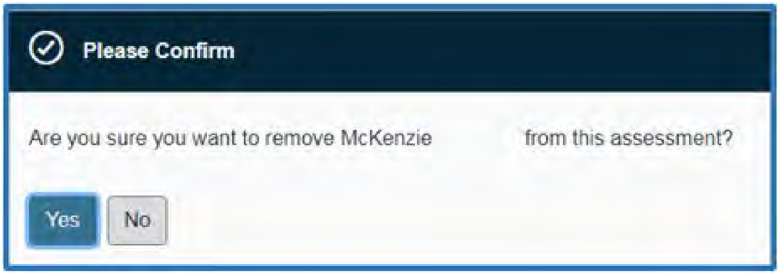
Your Username
Administrator
Assessment Owner

Test User
user@testing
User

Editing a Contact — Clicking the Change icon enables the contact text field to be editable so 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


Please Confirm

Are you sure you want to remove McKenzie from this assessment?

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

Inherent Risk Profiles

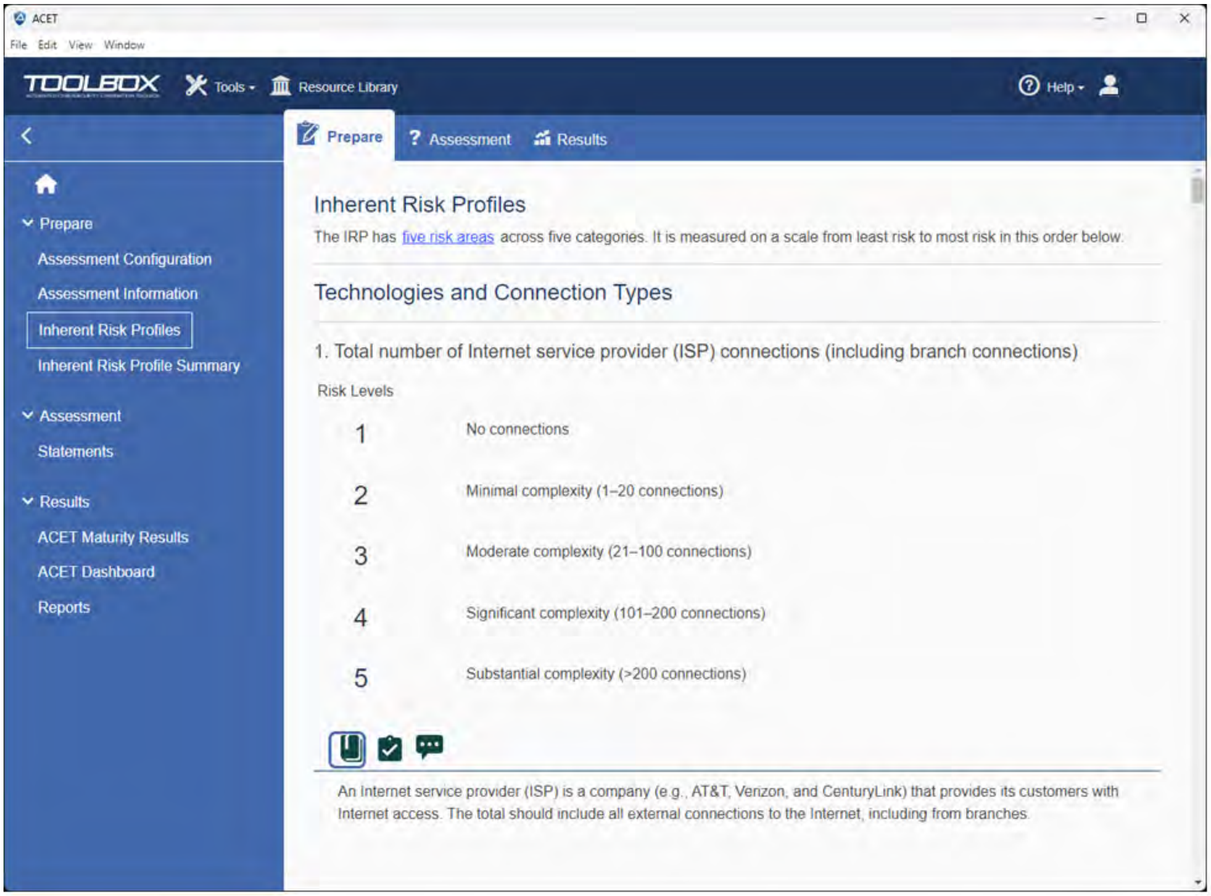
The IRP has five risk areas across five categories. It is measured on a scale from least risk to most risk in the order below:

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 or provided support documentation. There is often more than one way to verify responses.

Review the institution's IRP 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, see the ACET dashboard help section.

Figure: Inherent Risk Profile



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.

Technologies and Connection Types

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)

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.

IRP Categories — The IRP Categories break the IRP questions into groups.

IRP Questions — Users select Risk Levels for each individual IRP Question.

Risk Levels — The IRP has five risk areas across five categories. It is measured on a scale from least risk to most risk in the order below:

- **Least** — very limited use of technology.
- **Minimal** — limited complexity in terms of the technology it uses.
- **Moderate** — uses technology that may be somewhat complex in terms of volume and sophistication.
- **Significant** — uses complex technology in terms of scope and sophistication.
- **Most** — uses extremely complex technology to deliver myriad products and services.

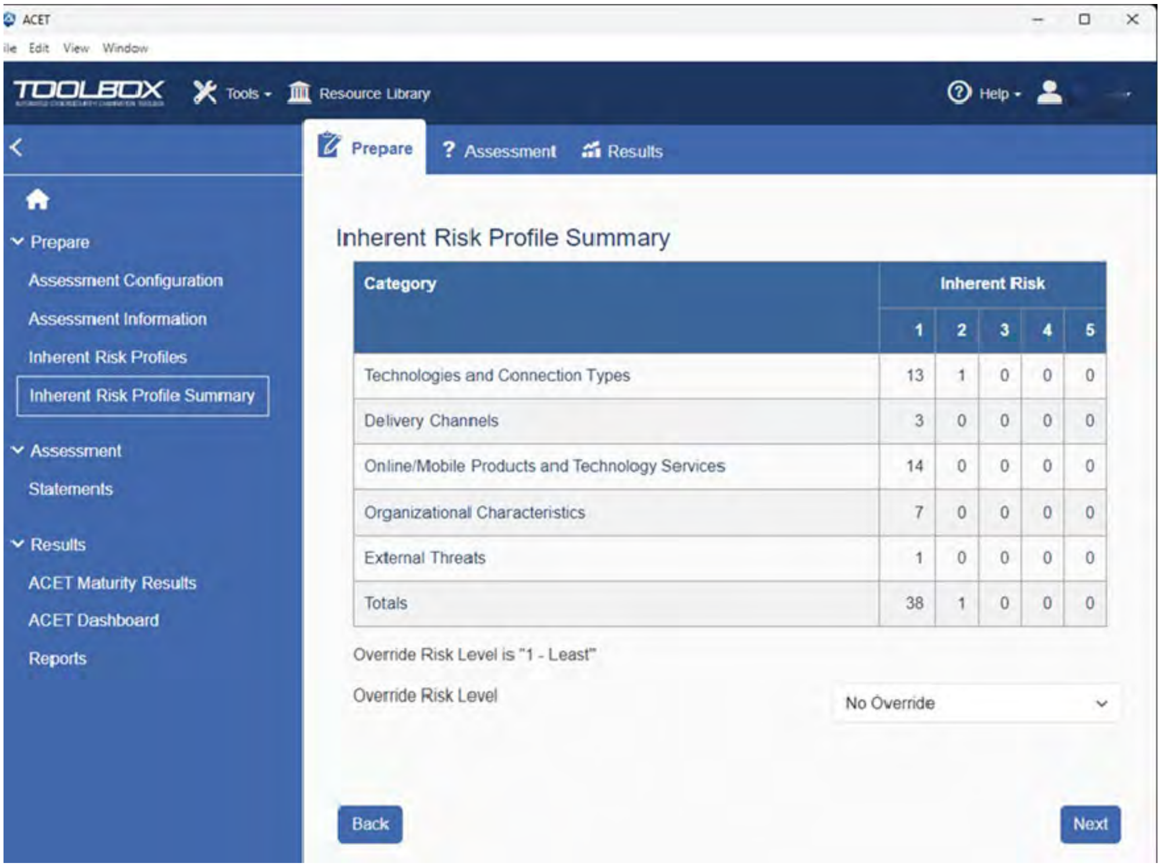
IRP Icons — The IRP icons are described in detail below.

- **IRP Description** 📖: The IRP Description gives added 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 on each IRP question.

Inherent Risk Profile Summary

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

Figure: IRP Summary



Inherent Risk Profile Summary

Category	Inherent Risk				
	1	2	3	4	5
Technologies and Connection Types	13	1	0	0	0
Delivery Channels	3	0	0	0	0
Online/Mobile Products and Technology Services	14	0	0	0	0
Organizational Characteristics	7	0	0	0	0
External Threats	1	0	0	0	0
Totals	38	1	0	0	0

Override Risk Level is "1 - Least"

Override Risk Level: No Override

You can use the Total Risk Level Override dropdown to override the 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 the ACET statements. The following sections will describe the Assessment process in detail.

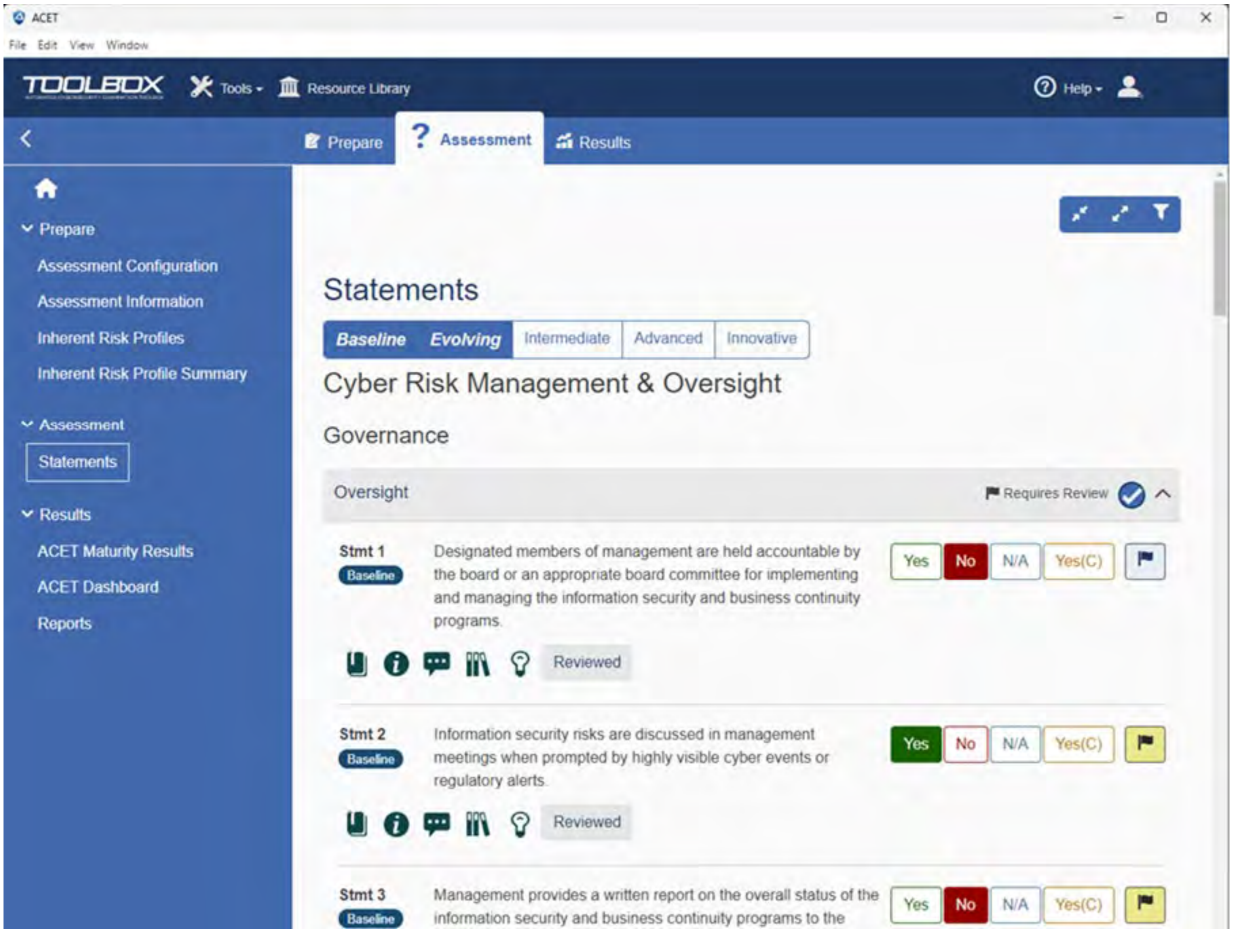
Assessment Screen

The primary interaction that takes place in the 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.

Most time will be spent completing the statements portion of the assessment. Although it is not difficult, the process of answering statements can be tedious. Users are advised to sufficiently prepare as it will take several hours —or even days—to accurately answer all the questions. The more time spent understanding each question's intent 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 during the assessment, comments can be associated with the relevant questions to document the activity.

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

Figure: Assessment Screen



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.

Stmt 2 Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.

Stmt 3 Management provides a written report on the overall status of the information security and business continuity programs to the

Cybersecurity Maturity Level Filter—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 italicized levels are within your range. To learn more, see the ACET Maturity Results section.

Domain Header — The domain header contains the component, assessment factors, and statements for the individual domain. In the example above, this is Cyber Risk Management and Oversight.

Component Header — The component header contains the assessment factors and statements for the individual component. In the example above, this is Governance.

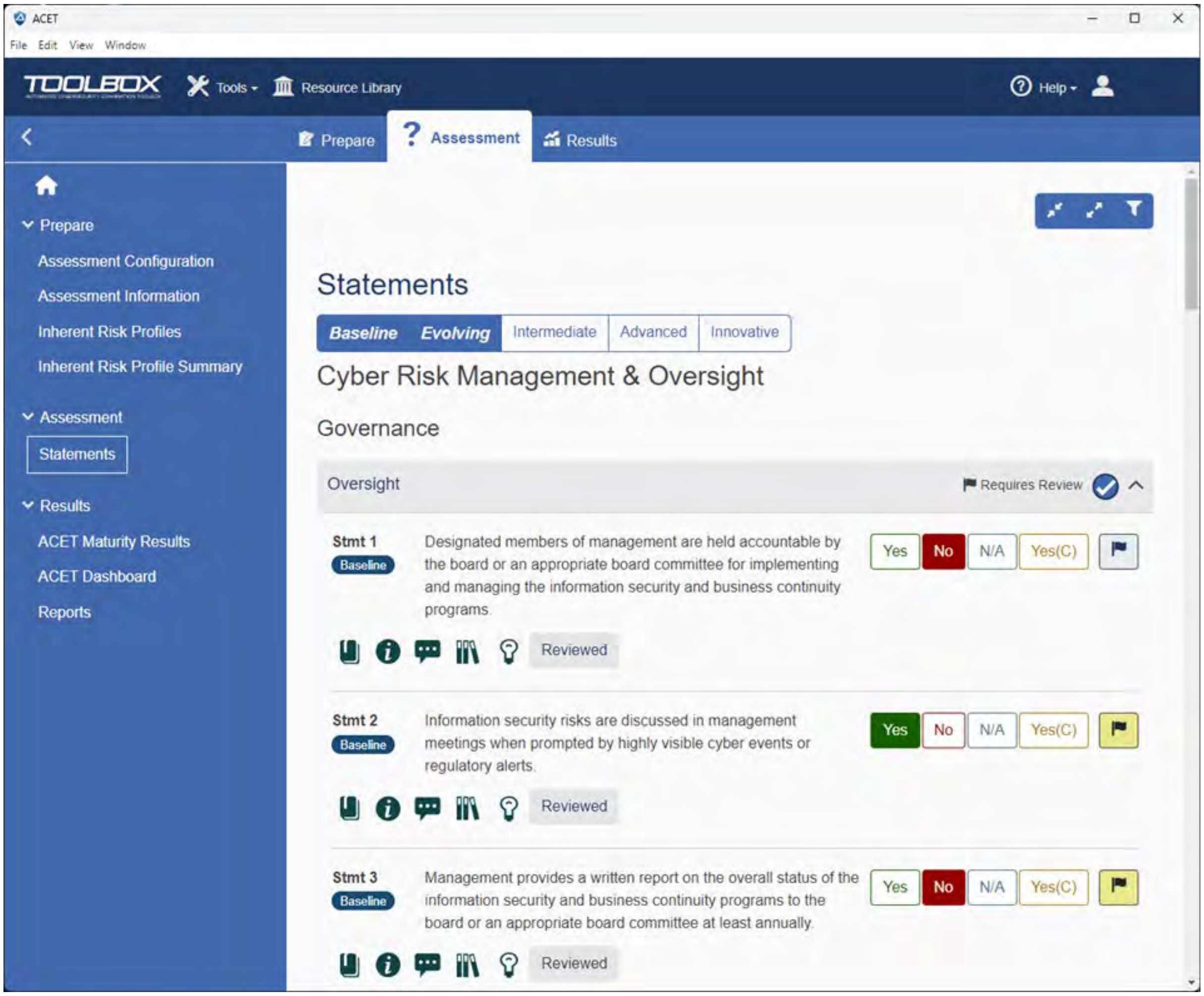
Assessment Factor Header — The assessment factor contains all statements for the individual assessment factor. In the example above, this is Oversight.

Statement Text — The Statement text contains the exact ACET statements. These are individually numbered.

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



Statements

Cyber Risk Management & Oversight

Governance

Oversight

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.

Stmt 2 Baseline — Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.

Stmt 3 Baseline — 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.

Collapse or Expand All — Click the Collapse All button to close all statement categories, and the Expand All button to open all statement categories.

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.

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.

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

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 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. This 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 like a Yes answer.

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.

Besides 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.

Mark for Review Button — The Mark for Review button allows you to mark a statement for future review.

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

Statement Icons — 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 the supplemental information for the statements. See the Supplemental Section for more information.

- **Comment 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.

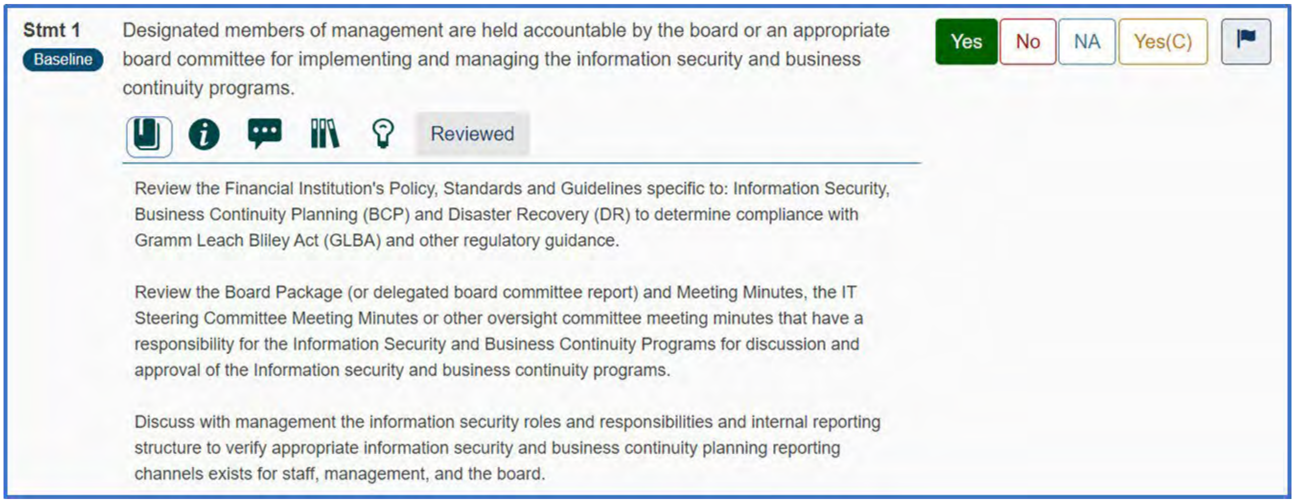
- **Observations Button** **:** clicking the observations button opens the observations section of the panel allowing you to create an observation record to associate with the statement. See the Observations Section for more information.

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

Exam Step

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

Figure: Exam Step



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.

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.

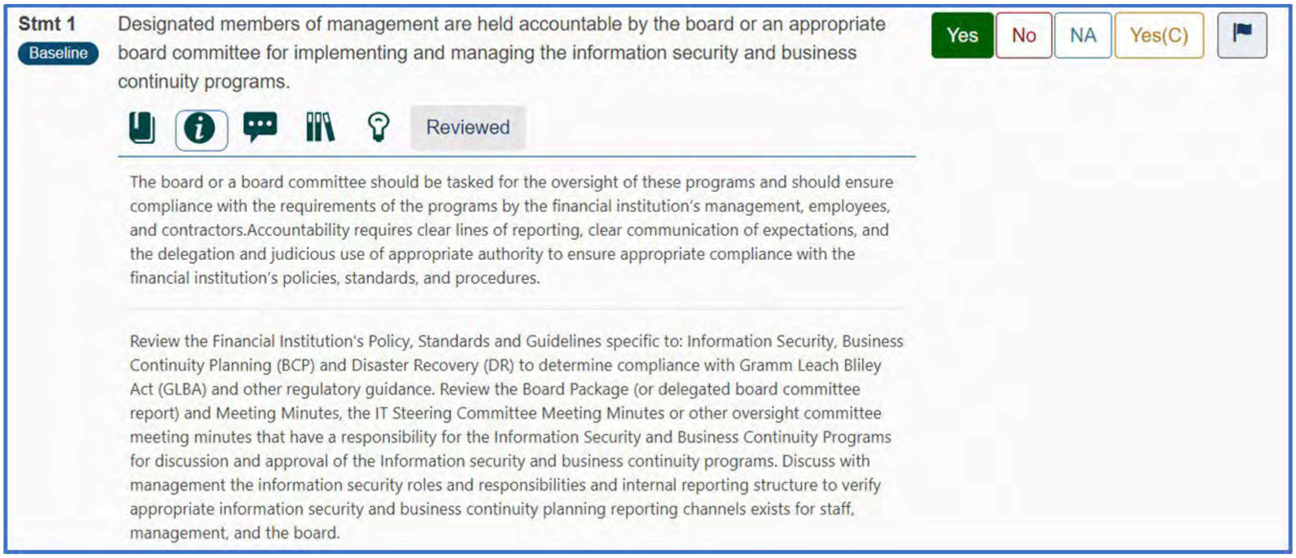
Review the Board Package (or delegated board committee report) and Meeting Minutes, the IT Steering Committee Meeting Minutes or other oversight committee meeting minutes that have a responsibility for the Information Security and Business Continuity Programs for discussion and approval of the Information 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.

Supplemental Section

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

Figure: Question Supplemental Information



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.

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.

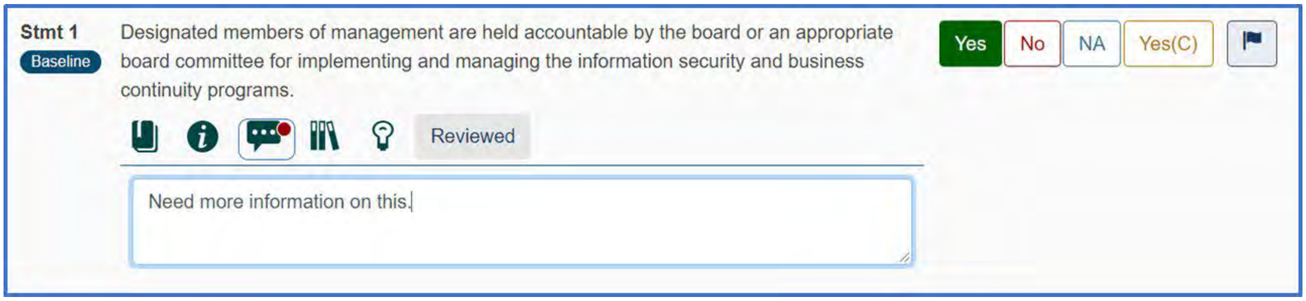
Review the Financial Institution's Policy, Standards and Guidelines specific to: Information Security, Business Continuity Planning (BCP) and Disaster Recovery (DR) to determine compliance with Gramm Leach Bliley Act (GLBA) and other regulatory guidance. Review the Board Package (or delegated board committee 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.

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. If they were not included in the Standard, there may be Statements that lack supplemental information. If a set of statements was taken from a single long requirement, the supplemental text may be repeated for multiple questions.

Comments Section

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

Figure: Assessment Screen Comments Section



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.

Need more information on this.

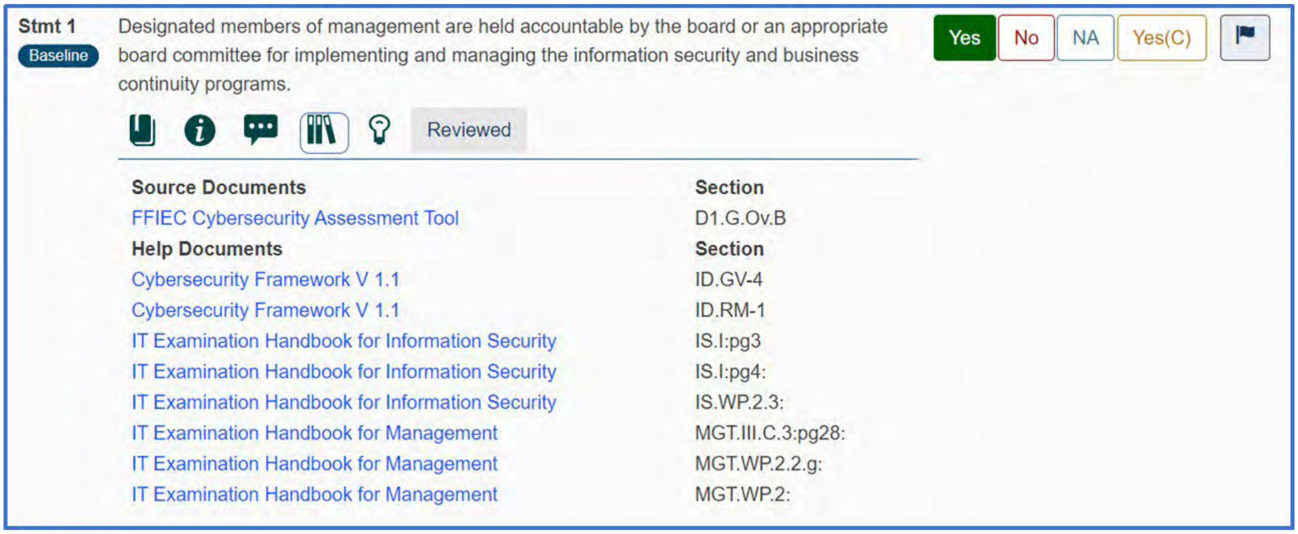
Comments Field — When a statement has comments, a red dot will be displayed on the comments button, enabling you to easily see which statements have comments as you scroll through the list of questions.

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 documents as seen in the figure below.



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.

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:

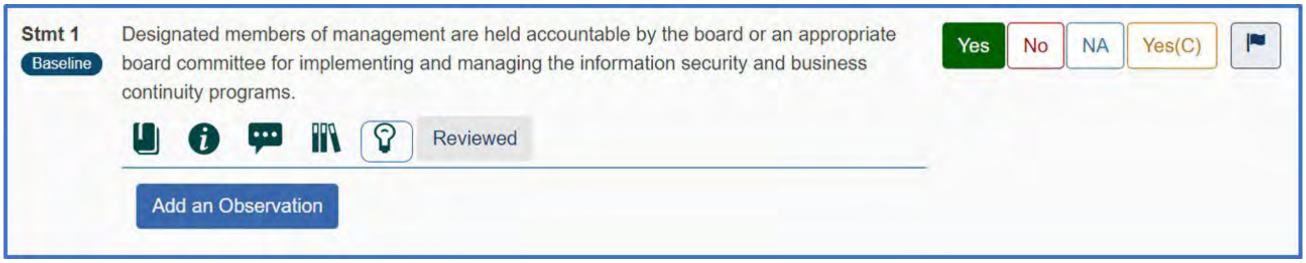
References Button — The references button displays all references related to the statement.

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

Observations Section

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

Figure: Observations section



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.

Observations Button — The observation button will display a red dot when the statement has associated observations. This allows you to easily see what statements have observations when scrolling through the list of questions.

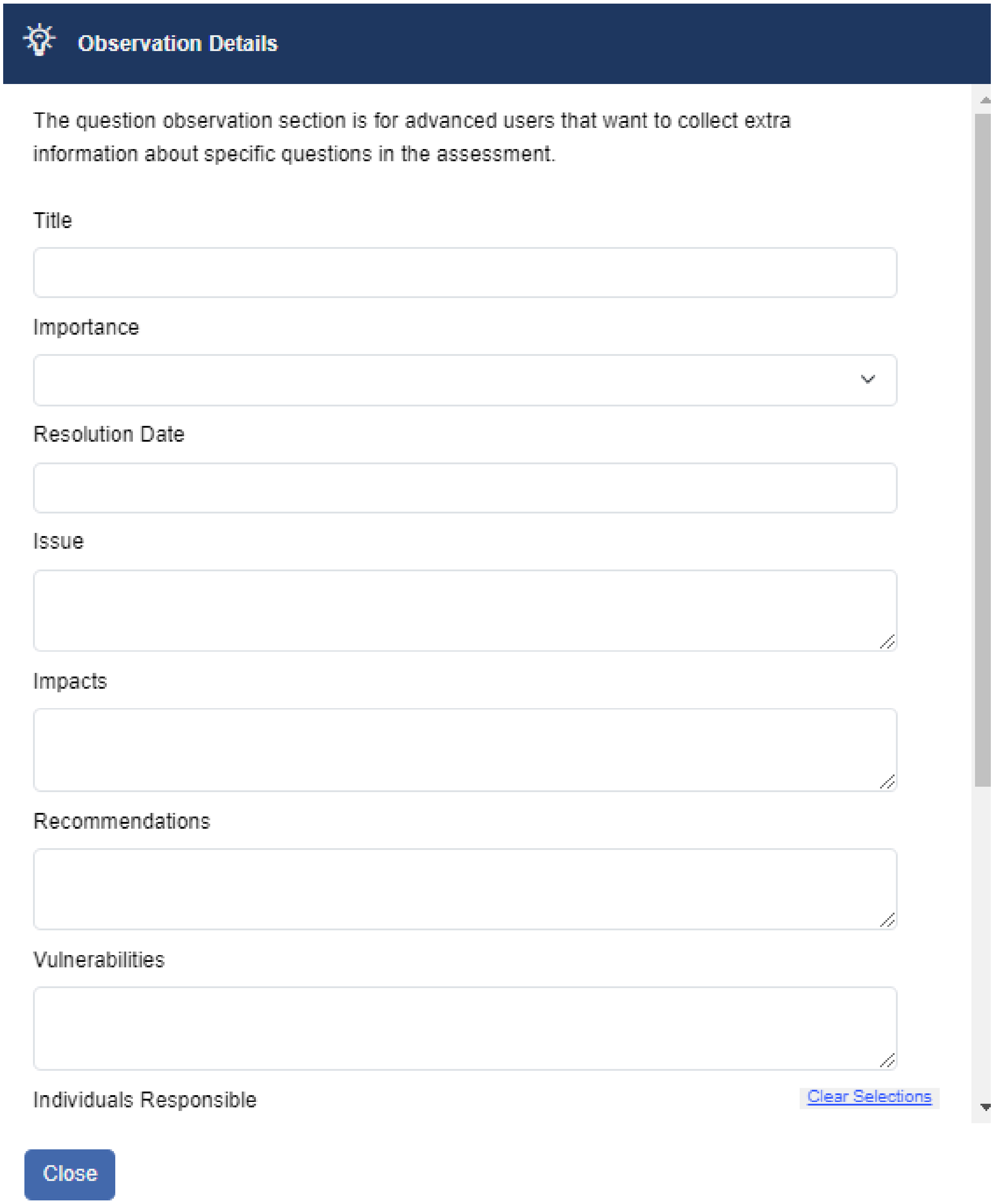
Add an Observation — Clicking the "Add an Observation" button opens the observations window that allows the user to enter all statement observation-related information.

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 record provides added information, potential impacts, recommendations for rectification, 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



Observation Details

The question observation section is for advanced users that want to collect extra information about specific questions in the assessment.

Title

Importance

Resolution Date

Issue

Impacts

Recommendations

Vulnerabilities

Individuals Responsible

Title — The observation title text box corresponds to a title or name for the observation record for easy identification.

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

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

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

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

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

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

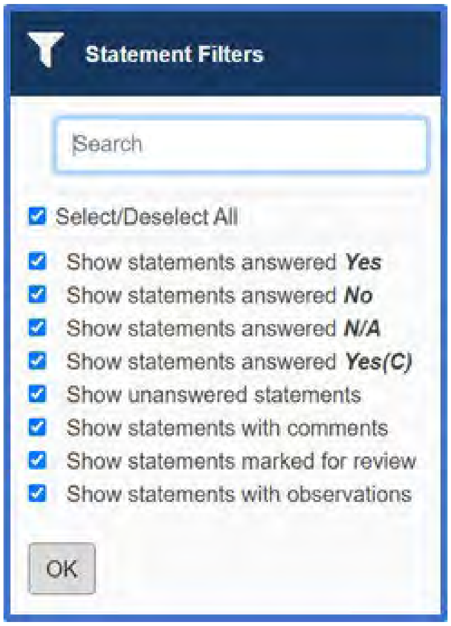
Individuals Responsible — The individuals responsible section allows you to assign individuals to be responsible for fixing the issues identified in the observation record. The contacts checklist will contain a list of all current contacts associated with the assessment. Selecting a contact will associate an individual to be responsible for the observation record. Add a contact in the contact window below, if the individual responsible is not in the current list.

Close — 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. The (C) in Yes (C) stands for compensating and shows the exact control has not been implemented, however, an added compensating control has.

Figure: Statement Filter



Statement Filters

Search

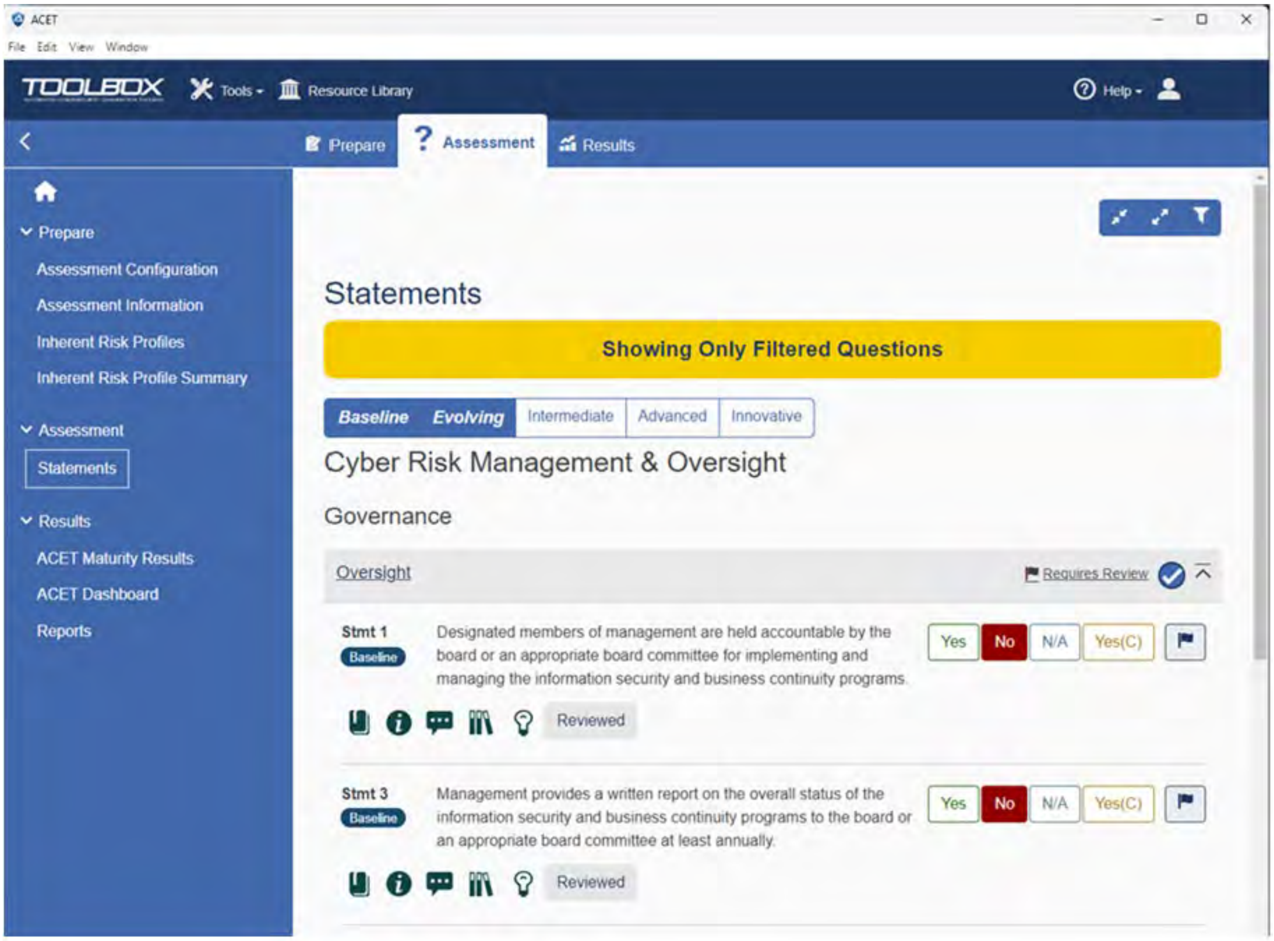
☑ Select/Deselect All

- ☑ Show statements answered ***Yes***
- ☑ Show statements answered ***No***
- ☑ Show statements answered ***N/A***
- ☑ Show statements answered ***Yes(C)***
- ☑ Show unanswered statements
- ☑ Show statements with comments
- ☑ Show statements marked for review
- ☑ Show statements with observations

You may select as many filters as you would like to combine, select all, or select none.

A message will appear if there are no results to show. You may then go back and change your selections as needed.

Figure: Showing only filtered statements



Statements

Showing Only Filtered Questions

Cyber Risk Management & Oversight

Governance

Oversight

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.

Stmt 3 Baseline — 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.

Results Section

Once you have completed answering statements, it is time to review and analyze the assessment results using two available methods. 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 the ACET Maturity Results, Dashboard, and Reports. This section will describe each area.

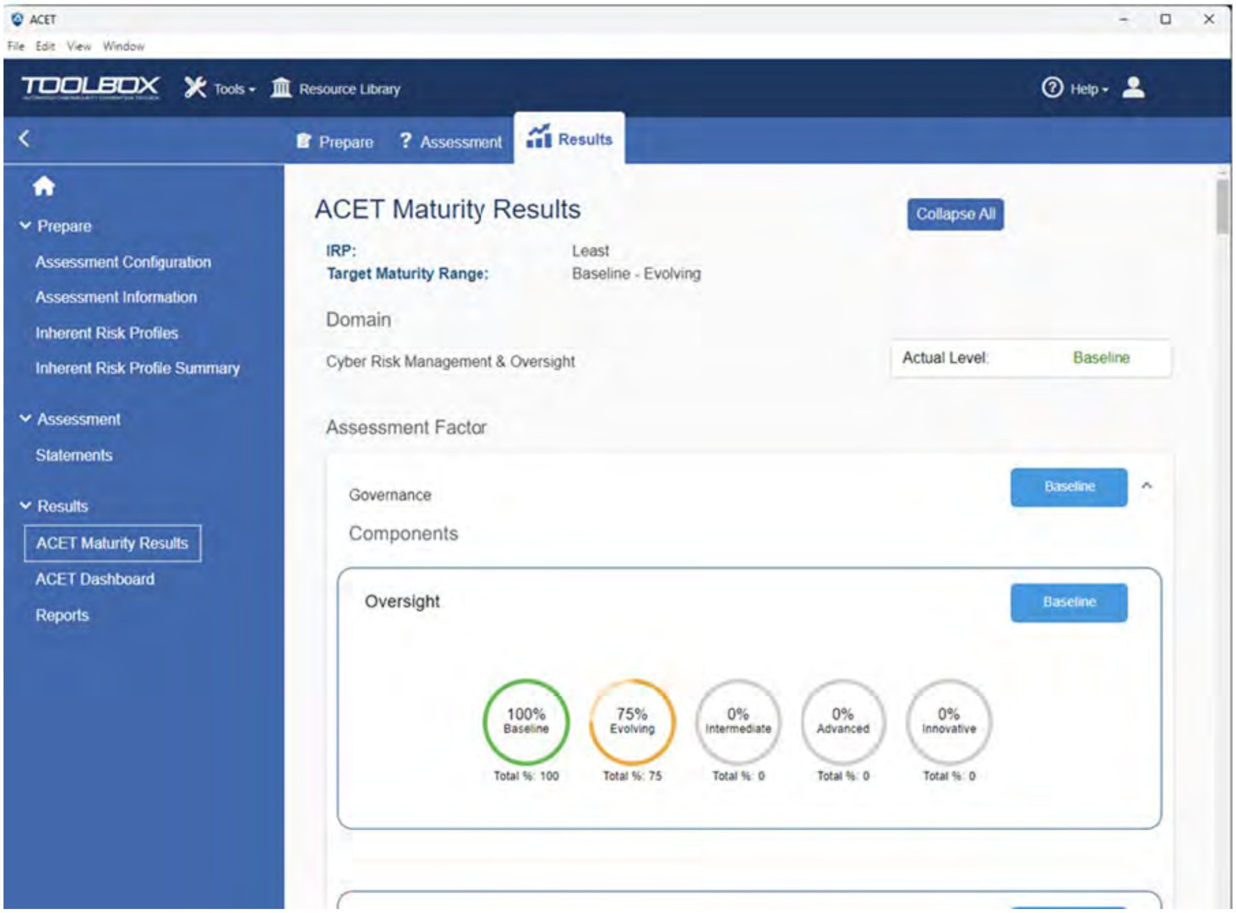
ACET Maturity Results

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 guide's 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 incomplete has not been completely answered. An item that has been fully answered but does not meet the baseline level is designated Ad Hoc.

Figure: Cybersecurity Maturity screen



ACET Maturity Results

IRP: Least
Target Maturity Range: Baseline - Evolving

Domain

Cyber Risk Management & Oversight

Actual Level: Baseline

Assessment Factor

Governance — Baseline

Components

Oversight — Baseline

100% Baseline	75% Evolving	0% Intermediate	0% Advanced	0% Innovative
Total %: 100	Total %: 75	Total %: 0	Total %: 0	Total %: 0

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

Target vs. Actual Level — 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.

Domain — 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 will remain incomplete.

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

Components — The components level 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 are defined below:

- Gray — Is not necessary for a user to answer based on their assigned level. Component levels that you do not need to answer are shown in gray.
- Red – 0% for assigned level. The levels that need to be answered, but have not been completed are shown in red.
- Yellow – 1-99% "No" answers do not count toward the percentage.
- Green — 100% of statements are answered.

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

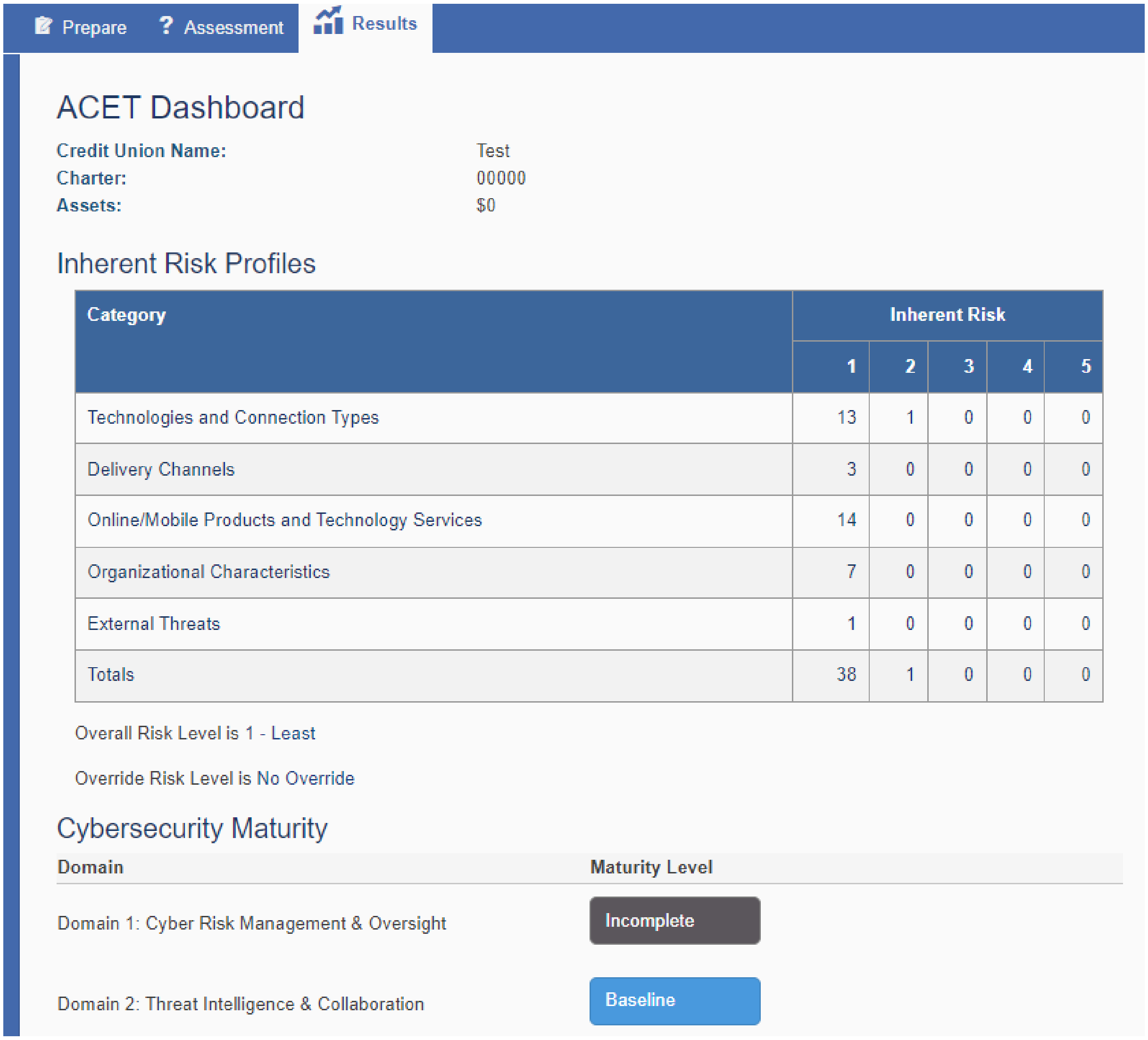
If it is red and says "Ad Hoc" then the statements have been fully answered but do not meet the Baseline level.

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.

Figure: ACET Dashboard



ACET Dashboard

Credit Union Name: Test
Charter: 00000
Assets: $0

Inherent Risk Profiles

Category	Inherent Risk				
	1	2	3	4	5
Technologies and Connection Types	13	1	0	0	0
Delivery Channels	3	0	0	0	0
Online/Mobile Products and Technology Services	14	0	0	0	0
Organizational Characteristics	7	0	0	0	0
External Threats	1	0	0	0	0
Totals	38	1	0	0	0

Overall Risk Level is 1 - Least

Override Risk Level is No Override

Cybersecurity Maturity

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

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:

- **Prepare section** — The Preparation section contains the demographic information noted on the Assessment Information section.
- **IRP section** — The IRP section repeats information found in the Inherent Risk Summary screen.
- **Cybersecurity Maturity Section** — The Cybersecurity Maturity section summarizes the maturity levels. The maturity levels will show as “Incomplete”

until responses for all the statements in the Baseline maturity for each Domain are complete.

Reports Section

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 to assign tasks to technical staff.

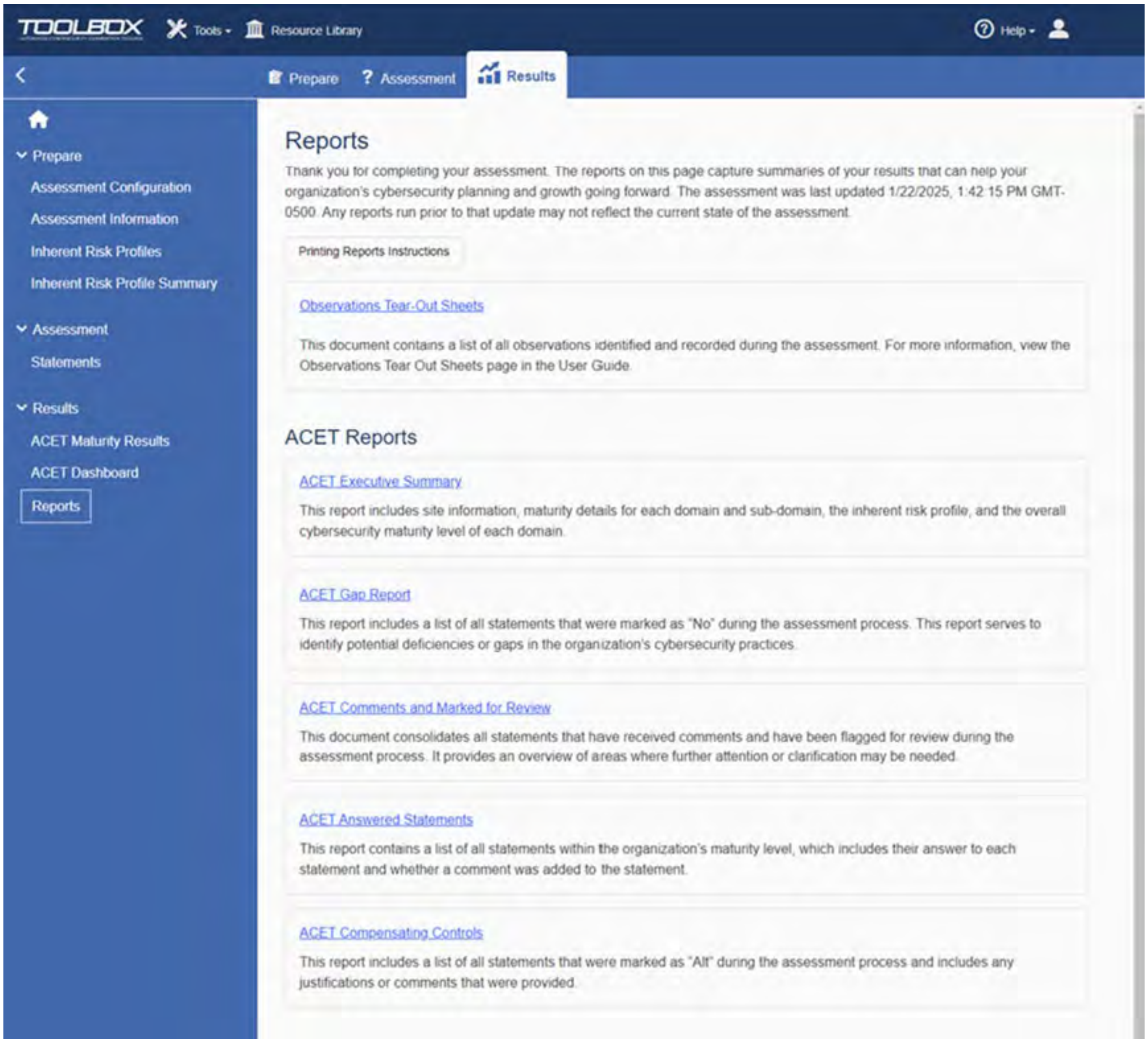
Combined with the online analysis, these reports can help to clearly understand where weaknesses are and where improvements should be made.

This section will describe how to use the Reports Screen after the assessment is completed.

Report Screen

The Report screen is shown in the figure below.

Figure: Report screen



Reports

Thank you for completing your assessment. The reports on this page capture summaries of your results that can help your organization's cybersecurity planning and growth going forward. The assessment was last updated 1/22/2025, 1:42:15 PM GMT-0500. Any reports run prior to that update may not reflect the current state of the assessment.

Observations Tear-Out Sheets

This document contains a list of all observations identified and recorded during the assessment. For more information, view the Observations Tear Out Sheets page in the User Guide.

ACET Reports

ACET Executive Summary

This report includes site information, maturity details for each domain and sub-domain, the inherent risk profile, and the overall cybersecurity maturity level of each domain.

ACET Gap Report

This report includes a list of all statements that were marked as "No" during the assessment process. This report serves to identify potential deficiencies or gaps in the organization's cybersecurity practices.

ACET Comments and Marked for Review

This document consolidates all statements that have received comments and have been flagged for review during the assessment process. It provides an overview of areas where further attention or clarification may be needed.

ACET Answered Statements

This report contains a list of all statements within the organization's maturity level, which includes their answer to each statement and whether a comment was added to the statement.

ACET Compensating Controls

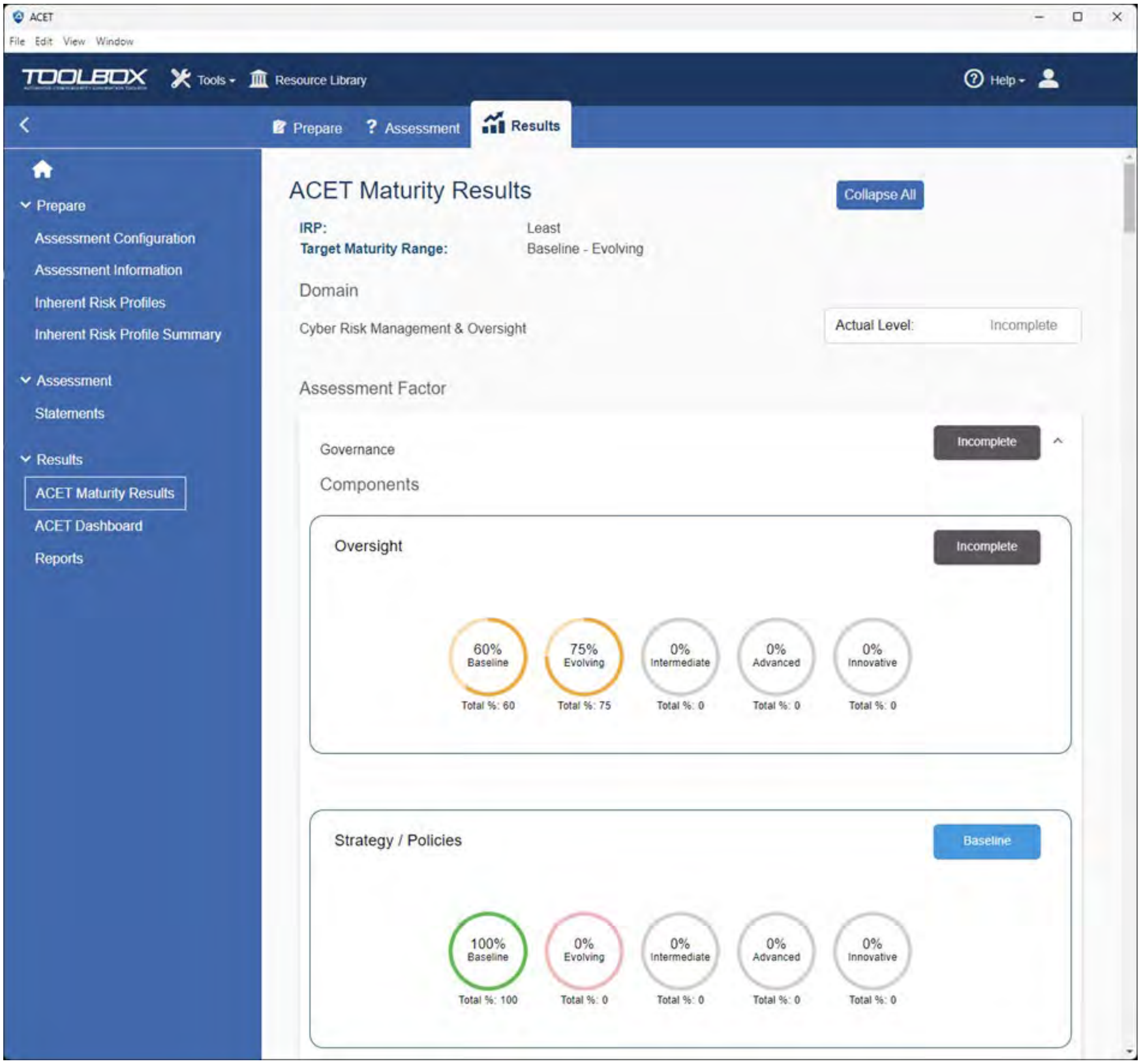
This report includes a list of all statements that were marked as "Alt" during the assessment process and includes any justifications or comments that were provided.

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, Gap Report, Comments and Marked for Review, Answered Statements, and Compensating Controls.

NOTE: Some reports will not be available if all statements within your target level have not been answered. The image below shows what the Report screen looks like if you have not completed your assessment.

Figure: Disabled Reports



IRP: Least
Target Maturity Range: Baseline - Evolving
Actual Level: Incomplete

Title Page — Each of the reports contain a cover page that is unique to the report type. These include 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 or Name field, and the Asset value entered in the Assessment Configuration screen.

ACET 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.

Site Information — Site Information includes all 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.

IRP — This screen is an output of the IRP Summary screen. It summarizes what you selected in the IRP 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.

ACET Gap Report

This report lists the statements that are "No" answers (gaps), any comments associated with the statement, and if it was marked for review. It is intended to assist the users of the report in identifying these gaps, prioritizing work, and 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. This means lower levels should be completed before moving to higher levels. Ideally, baseline should be completed before focusing efforts on controls in evolving and higher maturity levels.

ACET Comments and Marked for Review

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

- **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.

ACET Answered Statements

This report includes all the statements which is determined by your maturity range, your answers, and whether there is a comment attached to the statement.

- **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 with the Compensating Control.

ACET Compensating Controls

The Compensating Controls table shows each statement that was answered "Yes(C)", their associated compensating comments, and any added comments associated with the statement, and if it was marked for review.

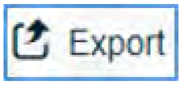
Export or Import an ACET Assessment

There are two different ways to import an ACET assessment. Pick an option below to learn more.

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

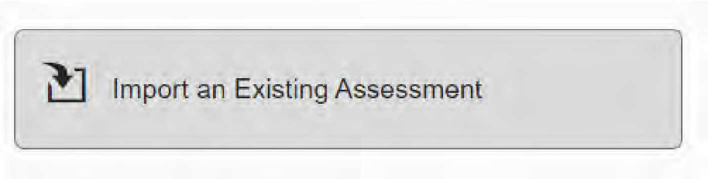


After clicking the Export button, the assessment will be downloaded as a .acet file and will be in the user's Downloads folder (unless otherwise specified in browser settings).

Importing a .acet File

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

Figure: Import Button



When the user's File Explorer opens, 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 the ACET only supports .acet file upload. Legacy file (.cset) upload is not supported.

Glossary

Acronyms

Acronym	Definition
ACET	Automated Cybersecurity Evaluation Toolbox
CHM	Compiled HTML files
HTML	Hyper Text Markup Language
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 do not meet the baseline level
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Most 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 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 five domains: • Cyber Risk Management and Oversight • Threat Intelligence and Collaboration • Cybersecurity Controls • External Dependency Management • 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.

Term	Explanation
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	The relative consequences of a successful attack against the control system being evaluated. The consequence analysis identifies the worst, reasonable consequence that could be generated by a specific threat scenario. The General SAL provides an overall rating of the criticality based on the users' review of security threat scenarios and estimated consequences. The SAL ranges from Low to Very High.
Security Categories	The security categories are related to the NIST 800-53 Standards and are defined as: CONFIDENTIALITY "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information. INTEGRITY "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information. AVAILABILITY "Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system. The NIST 800-53-related security categorizations of Low, Moderate, and High are explained as: LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Term	Explanation
	AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Maturity Level	The rating of High, Moderate, or Low for Confidentiality, Integrity, and Availability according to FIPS 199 and NIST SP800-60.
Supplemental	Supplemental provides more information to aid in answering statements.
Yes (C)	Yes Compensating. This is an answer option on the Statements screen.