CMMC Assessment Guide for CSET

The Cyber Security Evaluation Tool (CSET®), Version 10.2.

March 2021

The Cyber Security Evaluation Tool (CSET®) is developed by
the Cybersecurity & Infrastructure Security Agency (CISA).

Table of contents

1. Intro to the CMMC Model 3
2. CMMC - Quick Tutorial 4
3. CMMC Updates 5
4. Interview and Testing Components 6
5. CMMC Levels and Focus Areas 7
6. CMMC Practices 9
7. CSET Assessment Steps 10
    7.1. Prepare 13
    7.2. Assessment 16
    3.2. Results 26
    7.3. Reports 31

1. Intro to the CMMC Model

Cybersecurity Maturity Model Certification (CMMC)

CMMC stands for “Cybersecurity Maturity Model Certification” and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

The CMMC Assessment

In general, a maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. The content of such a model typically exemplifies best practices and may incorporate standards or other codes of practice of that discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its processes, practices, and methods and set goals and priorities for improvement.

The CMMC assessment process provides consistent guidance for assessing a contractor against a specific CMMC level.

CMMC Levels 1 through 3 consist of the security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Levels 1 through 3 also include an additional 20 CMMC specific- practices along with 3 CMMC maturity processes for each of the 17 CMMC domains.

CMMC Levels 4 and 5 include a subset of the enhanced security requirements from NIST SP 800-171B as well as other cybersecurity best practices and show that the contractor is capable of reducing the risk of Advanced Persistent Threats. As a contractor moves toward Level 5, they are required to standardize and optimize process implementation across the organization.

2. CMMC - Quick Tutorial

For an abbreviated guide to the basics of CSET's CMMC Assesssment, check out the CMMC Tutorial.

3. CMMC Updates

Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

DoD issued an interim rule, Assessing Contractor Implementation of Cybersecurity Requirements, on Sep 29, 2020 (effective Nov 30, 2020) to implement:

- The NIST SP 800-171 DoD Assessment Methodology
- The Cybersecurity Maturity Model Certification (CMMC) Framework

Additional Resources

- Assessing Contractor Implementation of Cybersecurity Requirements

Rule text at

- DFARS Case 2019-D041

NIST SP 800-171 DoD Assessment Methodology and Cyber/DFARS 252.204-7012 FAQs

- OUSD A&S (ASDA) - Defense, Pricing and Contracting Website

Using the Supplier Performance Risk System

For guidance relating to the use of the Supplier Performance Risk System (SPRS) in implementing DFARS CASE 2019-D014
Factsheet on DFARS Case 2019-D041

DoD Phased Rollout Plan for CMMC

The Department is implementing CMMC through a phased rollout approach. Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation.

The Department is currently working with military Services and Defense Agencies to identify candidate programs that will implement CMMC requirements during the FY2021-FY2025 phased rollout. During the first year of the rollout, the Department will require no more than 15 new Prime acquisitions to meet CMMC requirements as part of a CMMC pilot program. These contracts will focus on mid-sized programs that require the contractor to process or store CUI (CMMC Level 3). Primes will be required to flow down the appropriate CMMC requirement to their subcontractors.

For subsequent fiscal years of the rollout, the Department intends to incorporate CMMC Levels 4 and 5 on a small number of contracts while increasing the quantity of Prime acquisitions that include a CMMC requirement to the following targets:

FY2021	FY2022	FY2023	FY2024	FY2025
15	75	250	325	475

4. Interview and Testing Components

The Interview

An organization's assessor should have discussions with various individuals within the organization to understand if a practice has been addressed. Interviews of pertinent staff (often at different organizational levels) helps determine if practices are implemented and if adequate resources, planning, and training are available to help achieve CMMC goals.

Review of Assessment Objects

The assessor will review, inspect, observe, study and analyze documents, mechanisms, and activities. The assessor reviews documentation to determine if assessment objectives are met. Interviews with contractor staff may identify the documents the contractor uses. Documents must be final drafts; working papers (drafts) of documentation are not eligible as they are not yet official. Common types of documents that can be used as evidence include applicable:

- policy, process, and procedures
- training materials
- plans and planning documents
- system-level, network, and data flow diagrams

If a contractor doesn't have certain documents, other documents may be used to provide evidence.
In some cases, the practice is best assessed by viewing the safeguards in place for hardware, associated configuration information, or observing a process in action.

Demonstration and Testing

Testing is an important part of the assessment process. Interviews tell the assessor what the contractor staff believe to be true, documentation provides evidence of intent, and testing demonstrates what has or has not been done. For example, contractor staff may talk about how users are identified, documentation may provide details on how users are identified, but seeing a demonstration of identifying users provides evidence that the practice is met. The assessor will determine which practices, or objectives within a practice need demonstration or testing. Not all practices will require testing.

5. CMMC Levels and Focus Areas

The first step to completing the CMMC practice questions is to set your desired target level. If you are unsure of your target level, check your RFI or RFP documents for the required CMMC compliance level for your contract or choose your level based on the following guidance. Additional guidance on CMMC Levels can be found in the CSET Resource Library's collection of CMMC materials. Recommended reading includes the CMMC Model Certification 1.02 (March 2020), CMMC Assessment Guide: Level 1 v.1.10 (November 2021), and CMMC Assessment Guide: Level 2, v.1.10 (November 2021).

- Level 1: Safeguard Federal Contract Information (FCI)
- Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3: Protect Controlled Unclassified Information (CUI)
- Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

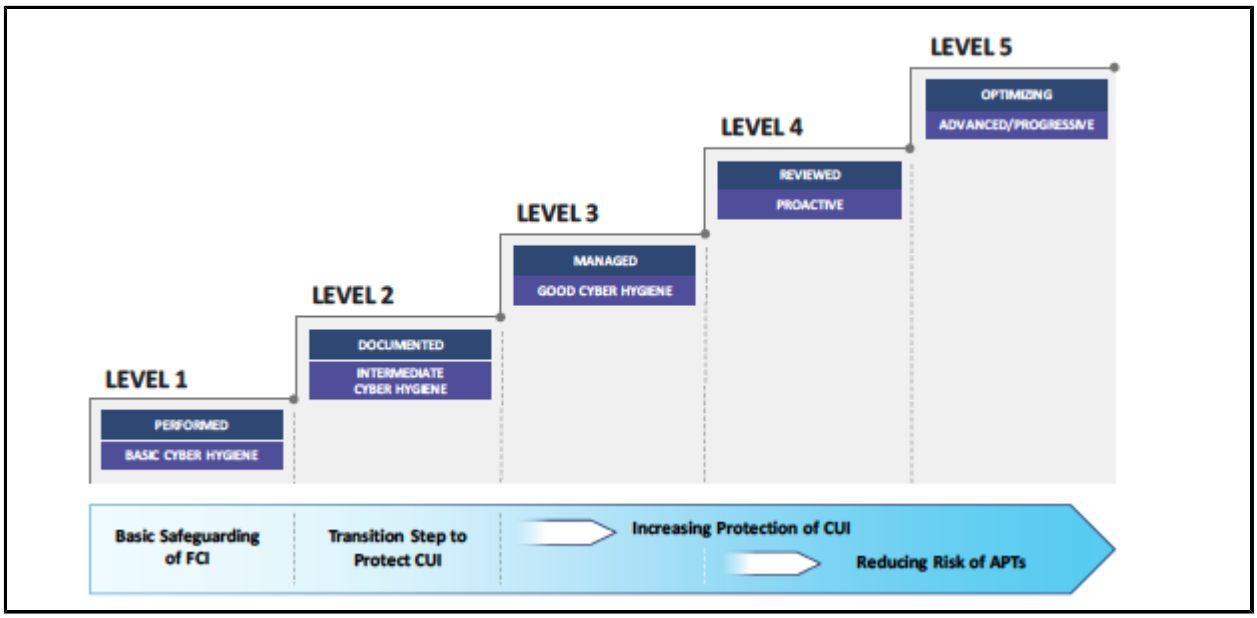


Figure 1: CMMC Levels and Associated Focus Areas

Level 1

Level 1 safeguards Federal Contract Information (FCI). Level 1 encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21, which defines FCI as:

Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Department of Defense (DoD) contracts that specify the need for a contractor to process, store, or transmit FCI only require the contractor to comply with CMMC Level 1 practices. There is no CMMC process maturity assessed at Level 1.

Level 2

Level 2 is a transitional level. At Level 2, a contractor is not yet approved for CUI. CMMC Level 2 practices and processes provide additional safeguarding above CMMC Level 1 and help to prepare a contractor to handle CUI at CMMC Level 3.

Level 3

CMMC Level 3 addresses the protection of Controlled Unclassified Information (CUI). The National Archives and Record Administration (NARA) defines CUI as:

Information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

A CMMC Level 3 assessment encompasses the practices and processes of CMMC Levels 1, 2, and 3. CMMC Level 3 shows that a contractor can adequately protect CUI at the appropriate risk level while accounting for subcontractor information flow in a multi-tier supply chain.

Level 4

Levels 4 provides increased assurance to the DoD that a contractor is capable of protecting CUI while working to reduce the risk of Advanced Persistent Threats and focuses on the protection of CUI from APTs. It encompasses cybersecurity best practices along with enhanced security requirements from NIST SP 800-171B . These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques,and procedures (TTPs) used by APTs.

Level 5

Level 5 continues the focus on the protection of CUI from APTs and requires a contractor to standardize and optimize process implementation across the organization.

6. CMMC Practices

The CMMC model measures not only process maturity or institutionalization, but also the implementation of practices. The model consists of 171 practices that are mapped across the five levels for all capabilities and domains. This mapping and the cumulative nature of the model is shown in Figure 2 below.

The CMMC Practices make up the individual questions in the CMMC Assessment.

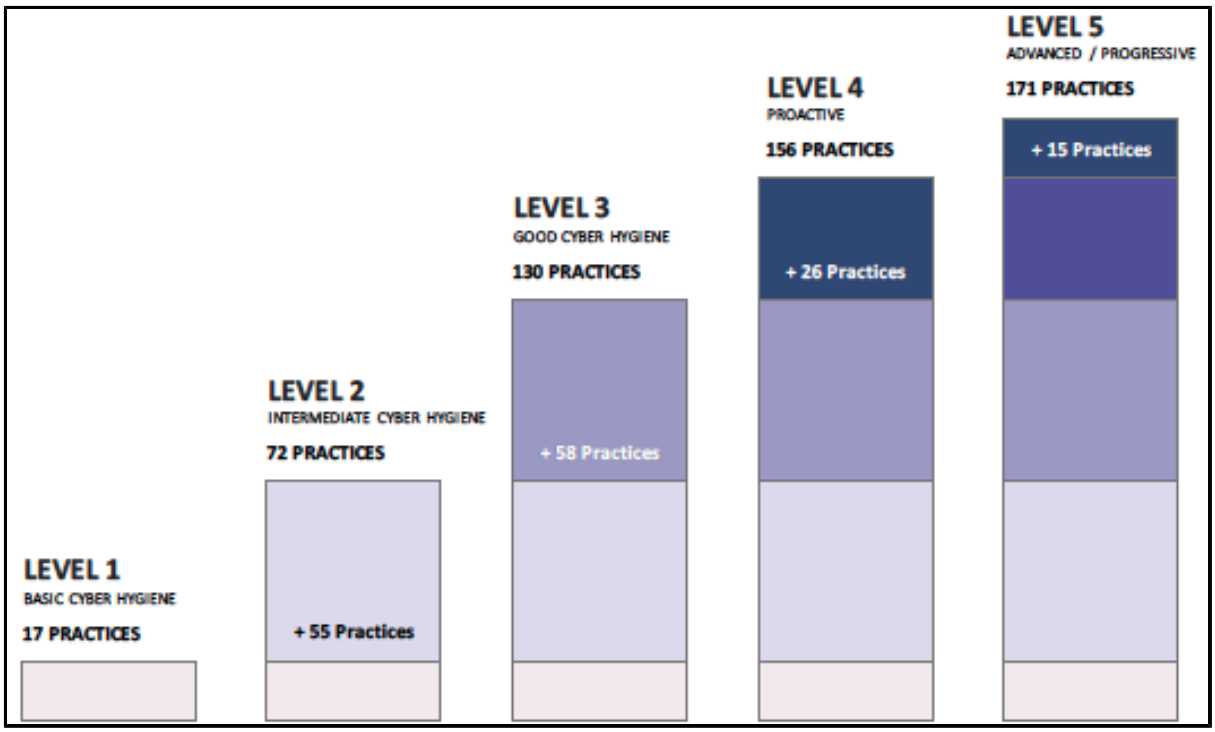
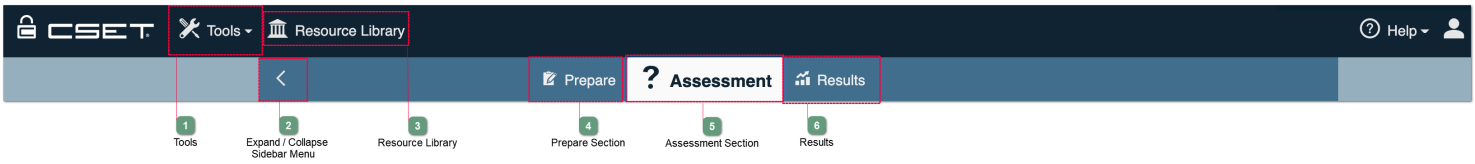


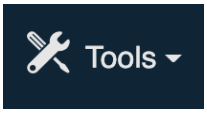
Figure 2: CMMC Levels and Associated Practices

7. CMMC Assessment Steps: Using the CSET Tool to complete a CMMC Assessment

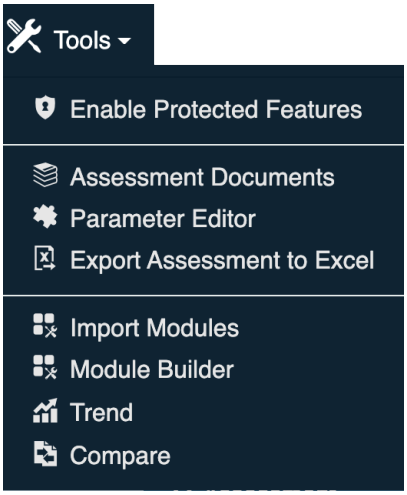
Note: The guidance below shows screen captures based on the Assessment tab in the Top Menu Bar selected.



1 Tools

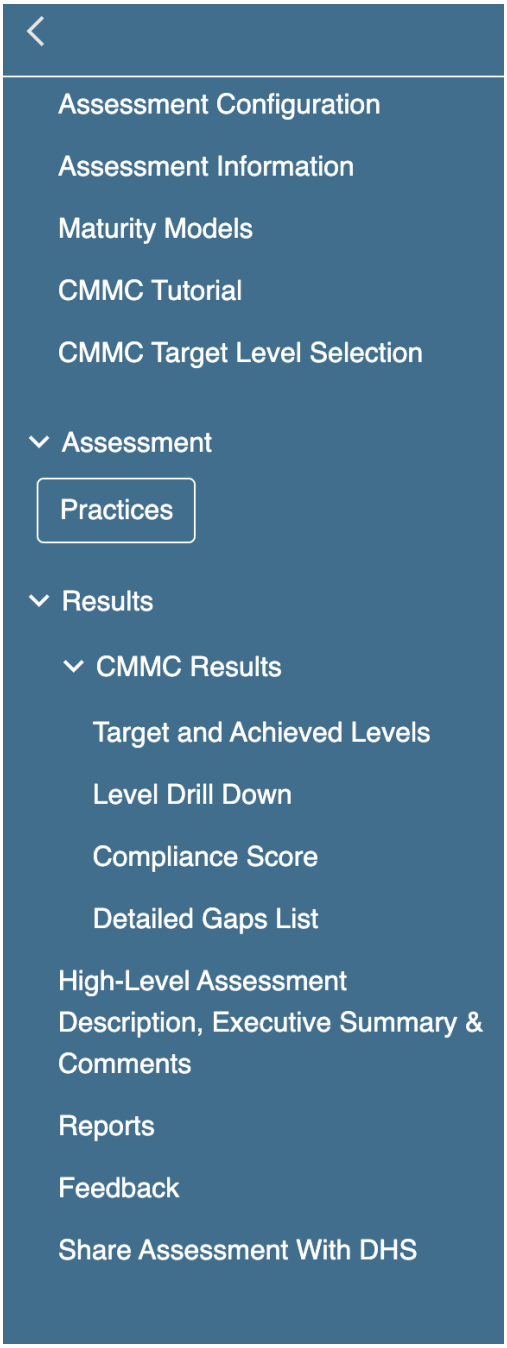


Selecting the drop-down Tools option expands the menu to show the following options. (For more detail on the Tools Menu options, visit the CSET User's Guide.)



2 Expand / Collapse Sidebar Menu

This function expands the Sidebar Menu which includes links to the following assessment features:



3 Resource Library

The Resource Library offers a collection of CSET's cybersecurity guidance documents and reference materials.

4 Prepare Section

The Prepare step is the first part of the assessment process and includes the following preparatory pages:

• The **Assessment Configuration** and **Assessment Options** fields to collect the user's information and assessment selections
• The **Assessment Information** screen where the user's basic demographic information is collected
• The remaining screens in the Prepare Step are tailored to the specifics of the user's Assessment Option choice

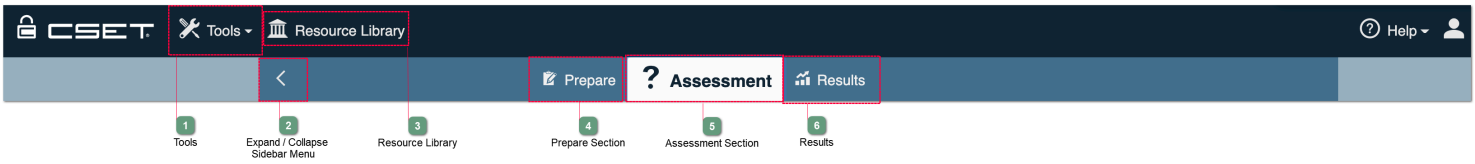
5 Assessment Section

Depending on whether the user has selected the Maturity Model, Standard, or Network Diagram, this section will display the **Maturity Model** selection page or the **Security Assurance Level (SAL)** selection page.

6 Results

The Results section details the various compliance metrics and measurements resulting from a completed assessment. The **Reports** section is located after the **Results** section in the **Sidebar Menu**.

7.1. Prepare



The Prepare step is the first part of the assessment process and includes the following preparatory steps

- The **Assessment Configuration** and **Assessment Options** fields to collect the user's information and assessment selections
- The **Assessment Information** screen where the user's basic demographic information is collected
- The remaining screens in the Prepare Step are tailored to the specifics of the user's Assessment Option choice

The Assessment Configuration Screen

The assessment user's organization information and assessment selections are collected.

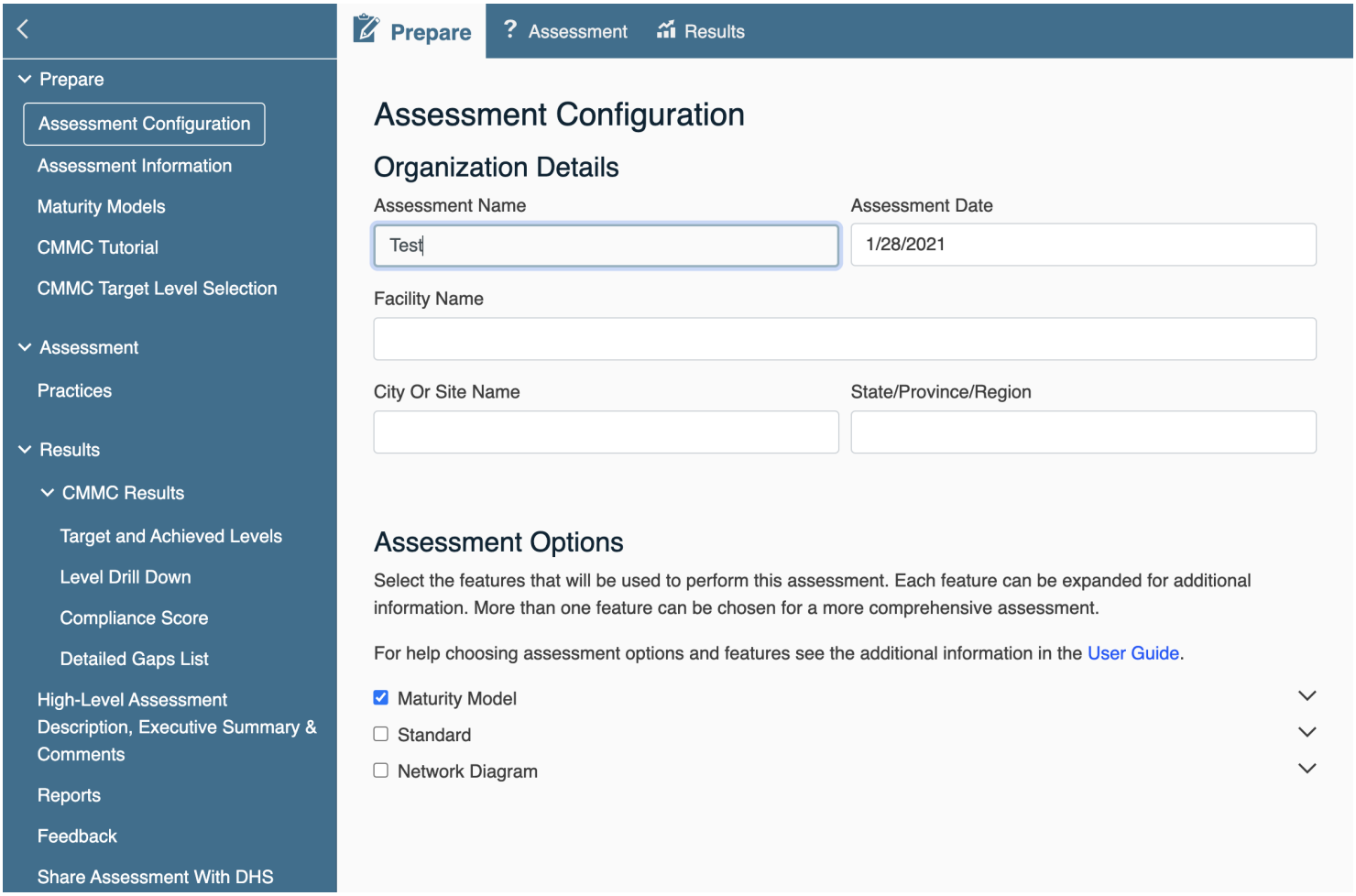


Figure: Assessment Configuration Screen

The Assessment Information Screen

Contact information is displayed and demographics information collected.

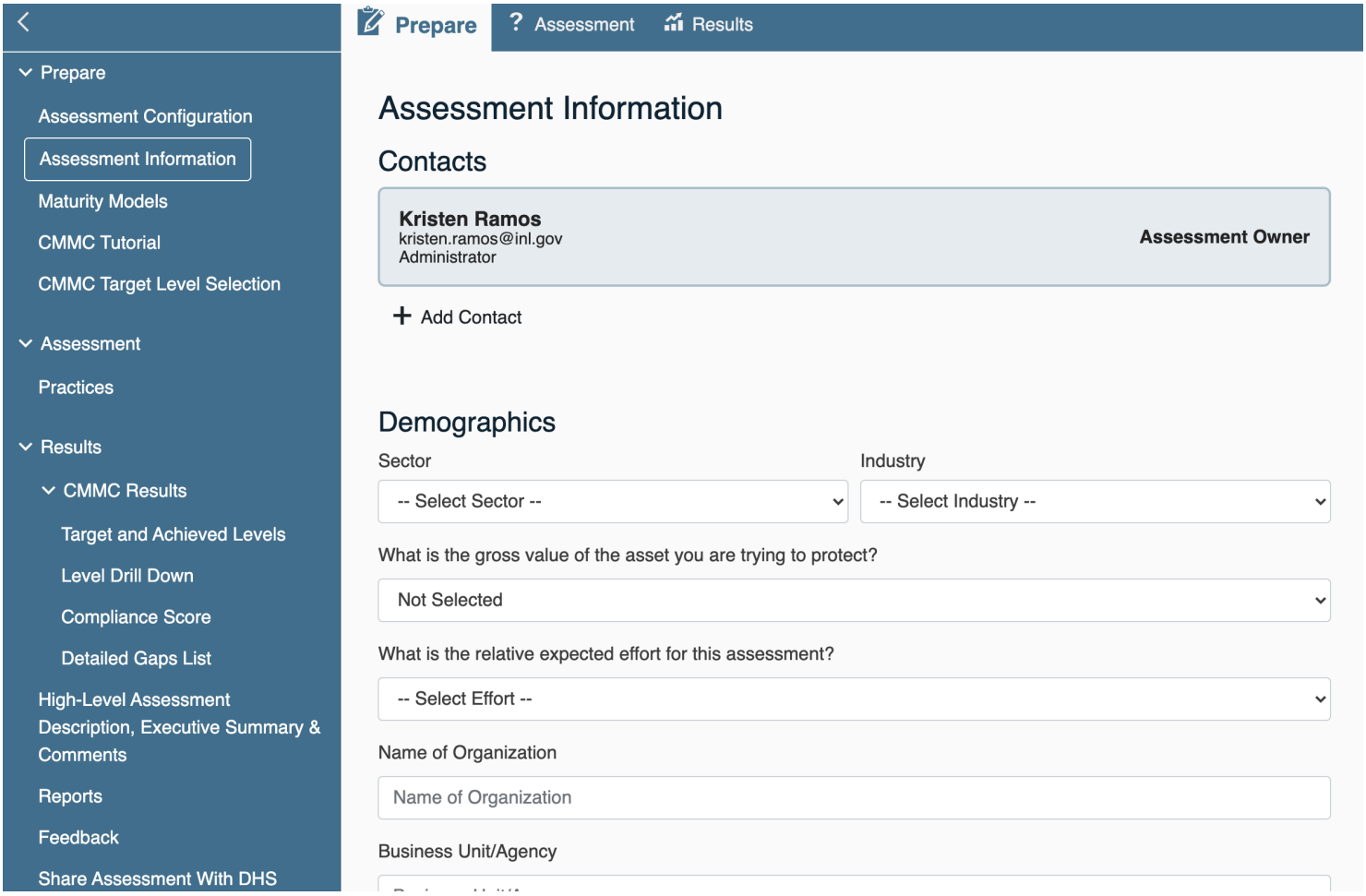


Figure: Assessment Information Screen

The Target Level Selection Screen

Select a target level via the target level bar at the top of the screen. CMMC target levels are cumulative, so selecting a level between 2-5 includes all levels below it. For more information and a description of each level, select the desired level from the target level bar to expand the text.

For help choosing a level, check the CMMC Levels section of this user guide. Users can also verify their required level on Requests for Information (RFIs) or Requests for Proposals (RFPs), as the DoD will specify the required CMMC level in the contract requirements.

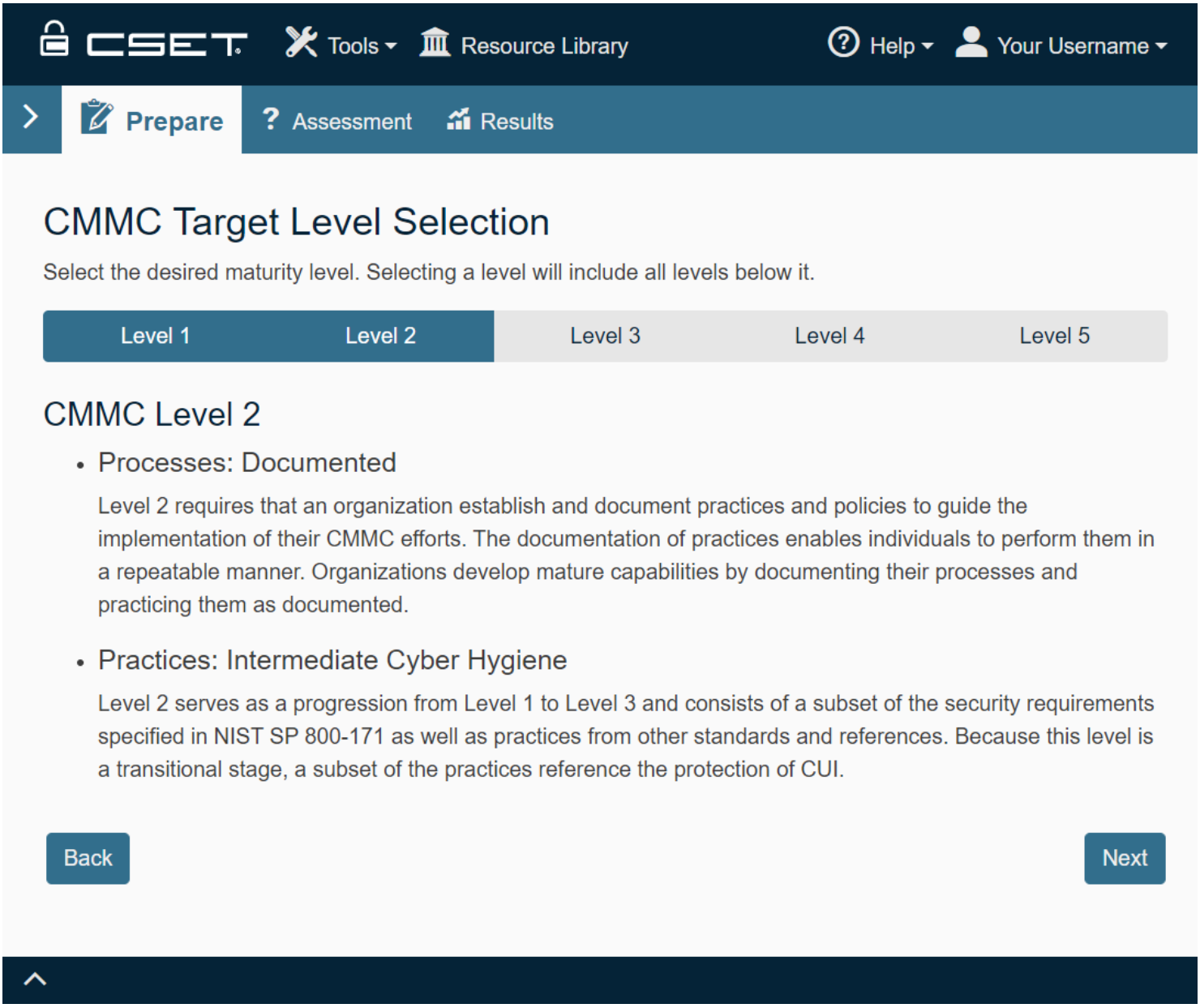


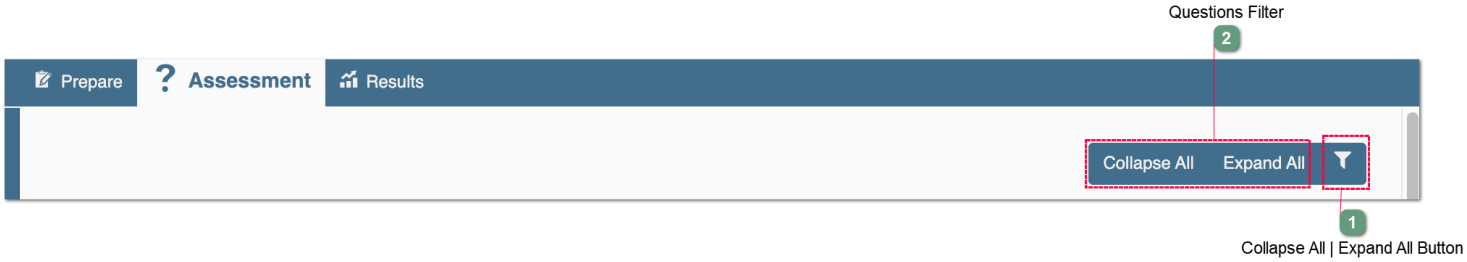
Figure: CMMC Target Level Selection screen

7.2. Assessment

1. Tailoring the Assessment

Filtering Practice Questions and Content on the Screen

Before starting the assessment, you may wish to tailor the content and questions you interact with.



To tailor your assessment, at the top right corner of the Assessment screen, note the 

buttons.

1 Collapse All | Expand All

While in the **Assessment Section** of CMMC, users can click the the **Collapse/Expand All** 

buttons at the top right of the screen to adjust wthe amount of practice questions content on the page.

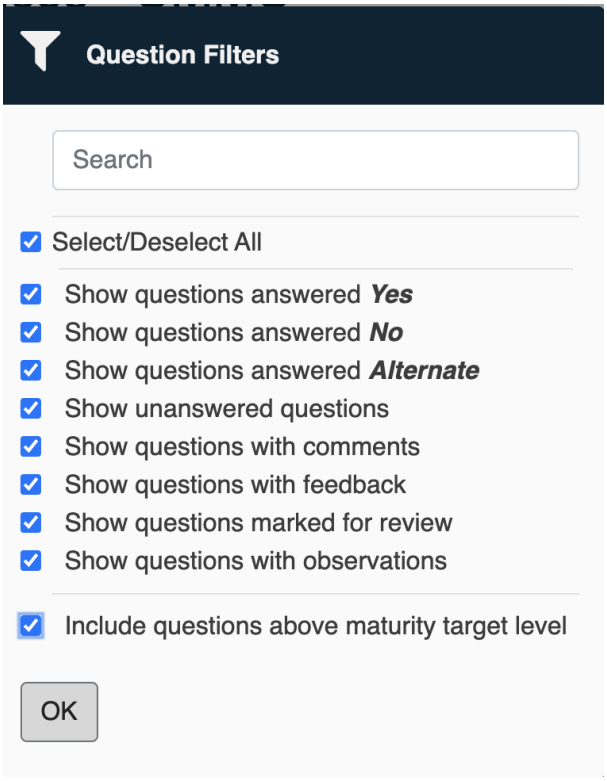
2 Questions Filter


The **Questions Filter** helps further tailor the types of content users interact with during the assessment.

Note: To View all CMMC Level Practice Questions Regardless of Target Level
In the Questions Filter pop-up screen (below) users can select the option to view questions above their set target level during the assessment. This will not affect the assessment target level scoring. Any additional questions answered beyond the user's selected target level will be shaded gray on the reports and not calculated in the final maturity score.

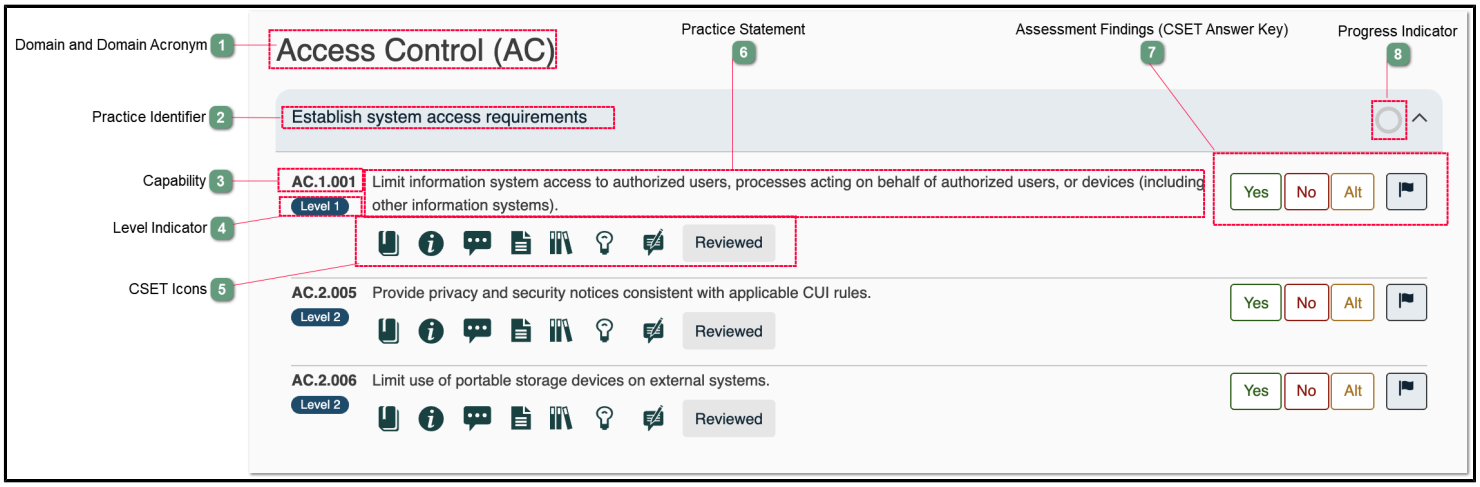
Questions Filter Pop-Up Screen

Select and de-select the checkboxes to tailor your practice questions throughout the assessment process. When you have finished the assessment, this feature is also useful during an on-screen assessment review.



2. Navigating the Assessment

CMMC Practice Question Layout



1 Domain and Domain Acronym

Access Control (AC)

The CMMC model consists of 17 domains. The majority of these domains originate from the security-related areas in Federal Information Processing Standards (FIPS) Publication 200 and the related security requirement families from NIST SP 800-171. The CMMC model also includes the three domains of Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

2 Practice Identifier

AC.1.001

Each CMMC practice is specified using the convention of **[DOMAIN].[LEVEL].[PRACTICE NUMBER]**

3 Capability

Establish system access requirements

There are 43 capabilities associated with the 17 domains in the CMMC model.

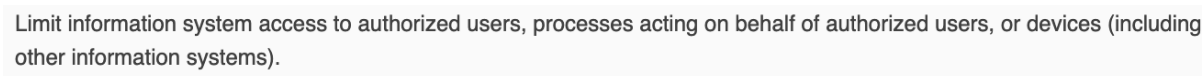
4 Level Indicator

Indicates the corresponding level associated with the practice statement. CMMC provides a benchmark against which an organization can evaluate the current **level** of capability of its processes, practices, and methods and set goals and priorities for improvement.
The CMMC assessment process provides consistent guidance for assessing a contractor against specific CMMC **Levels 1-5.**

5 CSET Icons

In the **CSET Icons** section below, you will find a breakdown of each of the CSET-specific icons and how they help facilitate a CMMC assessment.

6 Practice Statement



The CMMC model consists of 171 practices that are mapped across the five levels for all capabilities and domains. This mapping and the cumulative nature of
the model is shown in Figure.

7 Assessment Findings (CSET Answer Key)

A full breakdown of the CMMC Assessment Findings (CSET Answer Key) is below.

8 Progress Indicator

The Progress Indicator will turn blue and complete the circle as the questions in each Capability area are completed. When all the questions are complete, the Progress Indicator will show a check mark.

3. CMMC Practice Identifiers

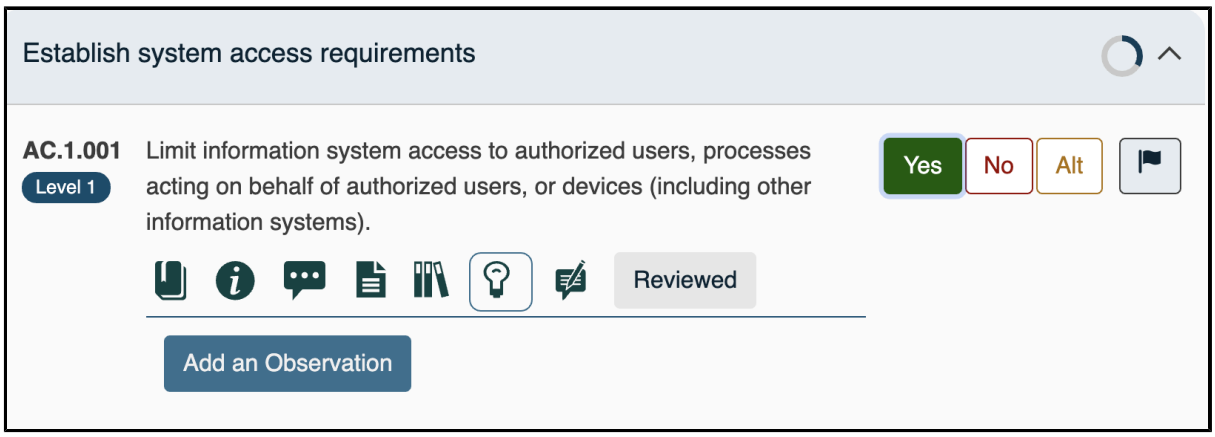
Each practice is specified using the convention of **[DOMAIN].[LEVEL].[PRACTICE NUMBER]** above the applicable **level number** for the practice.

- **DOMAIN** is the two letter domain abbreviation;
- **LEVEL** is the level number; and
- **PRACTICE NUMBER** is the identifier assigned to that practice.
- **Level 1, 2, 3, 4, or 5.**

4. CMMC Answer Key Structure

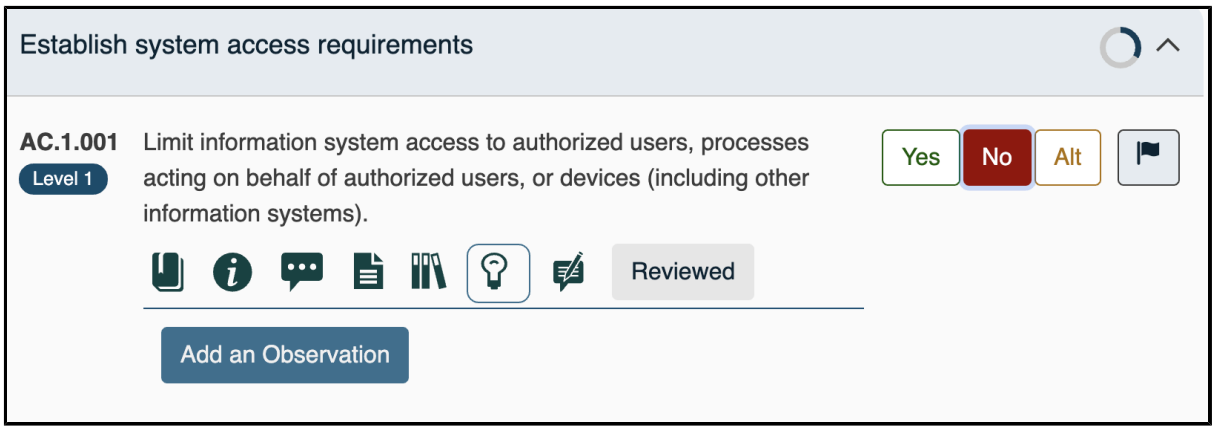
Yes **MET** is presented as **Yes** in the CSET Assessment Tool. The contractor successfully meets the practice. For each practice marked MET, the assessor includes statements that indicate the response conforms to the objectives and documents the appropriate evidence to support the response.

For **MET (Yes)**, the assessor can use the **Observations** field to record applicable observations.



No **NOT MET** is presented as **NO** in the CSET Assessment tool. The contractor has not met the practice. For each practice marked NOT MET, the assessor includes statements that explain why and documents the appropriate evidence that the contractor does not conform to the objectives.

For **NOT MET (No)**, the assessor can use the **Observations** field to record applicable observations.

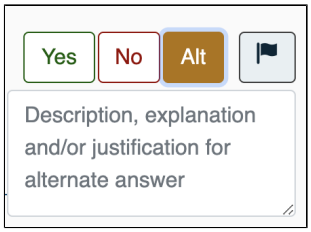


Inherited Practice Objectives - MET

Note: A contractor can inherit practice objectives. A practice objective that is inherited is met because adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice.

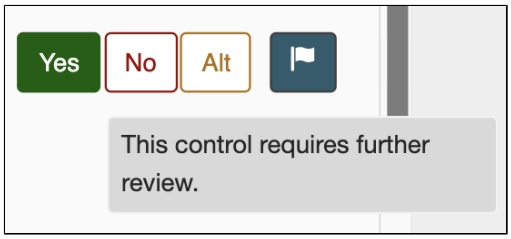
NOT APPLICABLE is presented as **ALT** n the CSET Assessment Tool. ALT indicates the practice does not apply for the assessment. For each practice marked ALT, the assessor is required to include a statement that explains why the practice does not apply to the contractor.

Assessor comments can be recorded in the pop-up alternate justification text box beneath the question.



Flag for Review

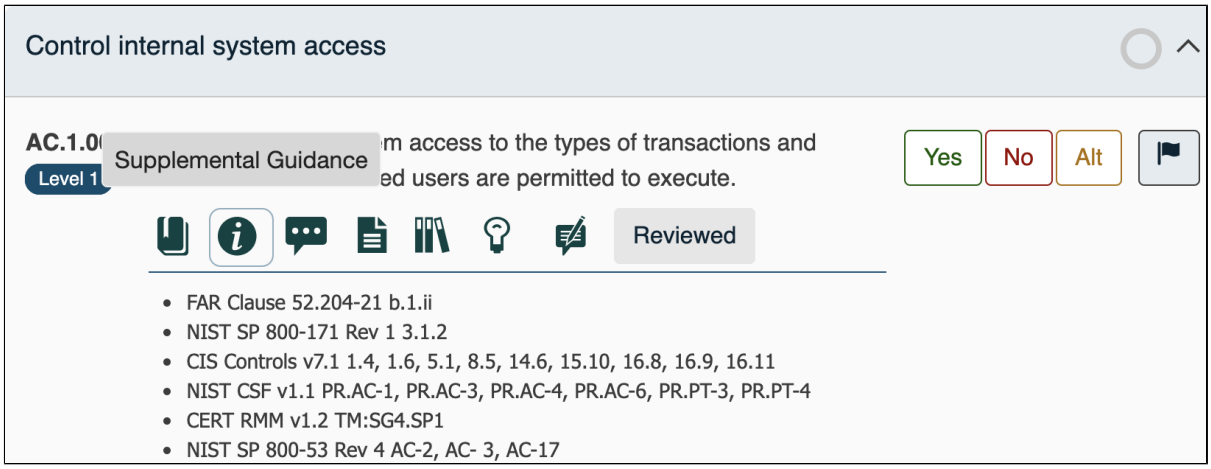
The flag for review function allows a user to mark a practice question for further review.



5. CMMC Icon Components

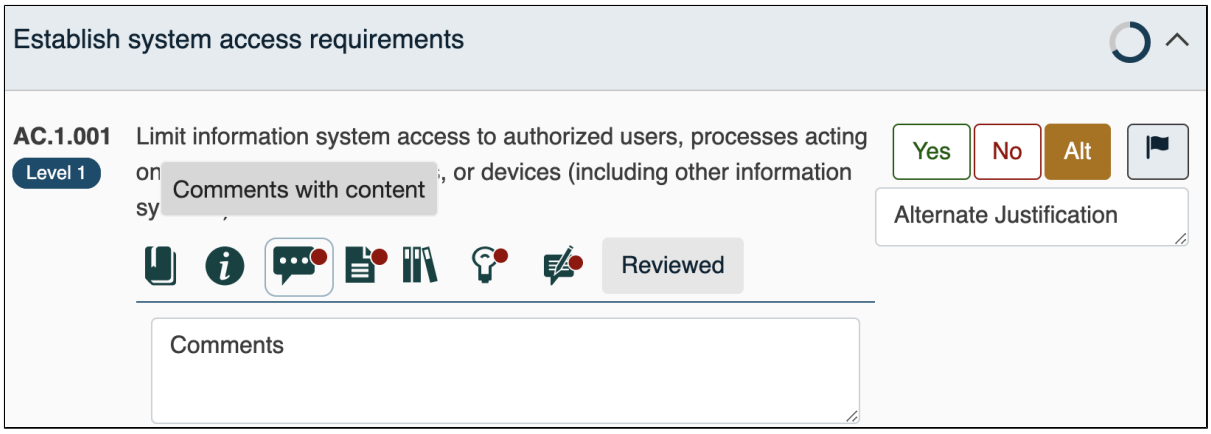
Supplemental Guidance

Users can refer to the supporting authorities and additional guidance provided under **Supplemental Guidance**. Many of these documents can be found in the [CSET Resource Library.]



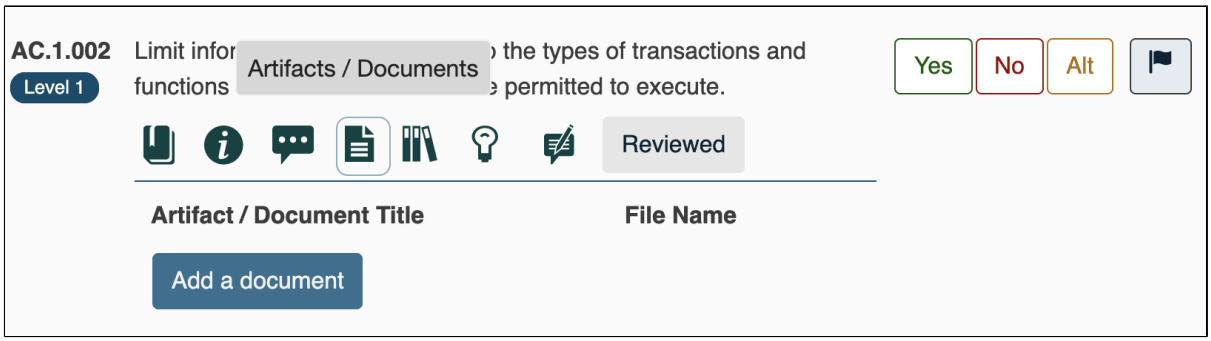
Comments

The comments function allows the assessor to record non-structured comments for each question during the assessment. In contrast, the Observations function (also useful for commenting) is more rigid and contains required fields.



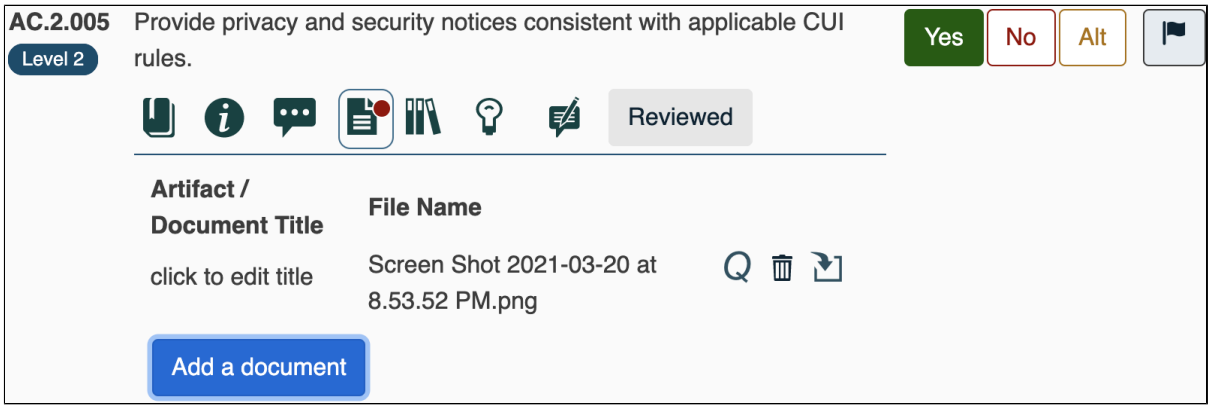
Artifacts/Documents

Assessors can use the Artifacts/Documents function to attach relevant evidence to each practice question.



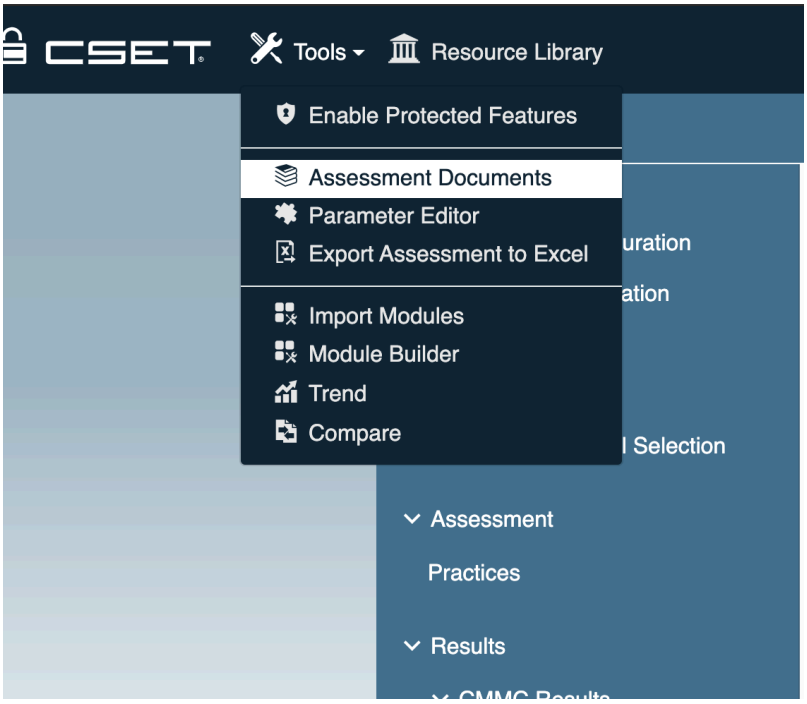
Attached Artifacts/Documents

The documents will appear listed by file name beneath the question when attached. A red indicator will appear on the icon for each question where evidence has been attached.

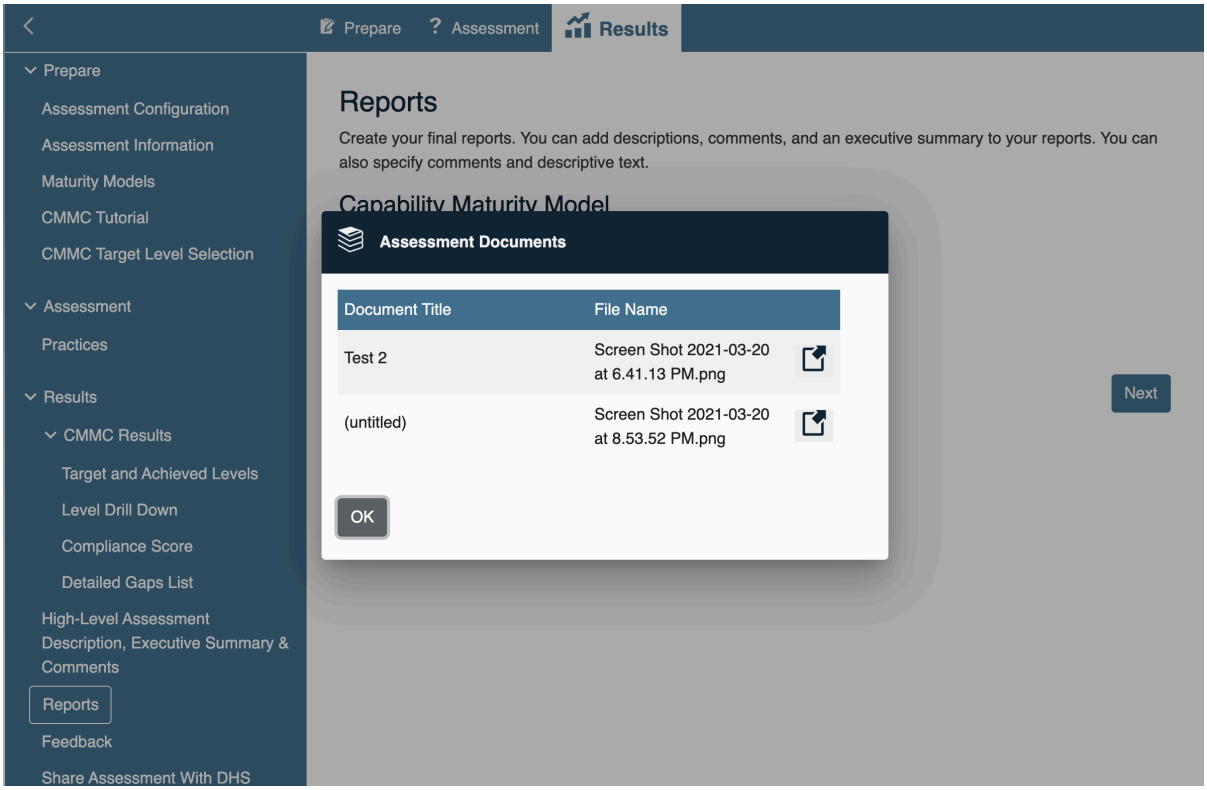


Attached Documents Storage

Access your attached documents, artifacts, and evidence under the  Tools Menu next to the CSET Logo on the upper left side of the screen.

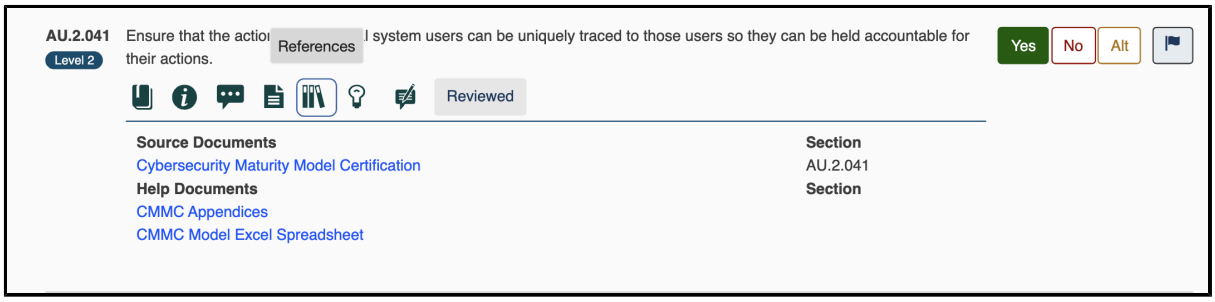


The Assessment Documents tab will open up a pop-up window showing all documents that are attached to the Assessment. Documents are organized by title.



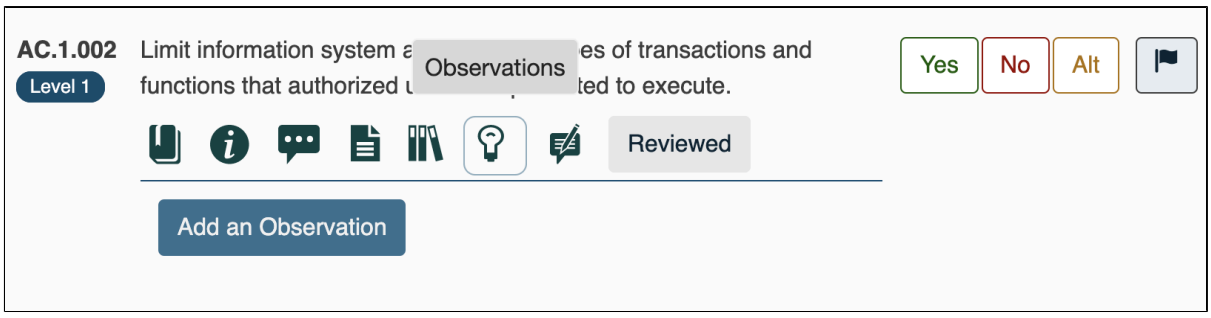
References

Users can click on the **References** icon to open links to CMMC .pdf documentation and to access CMMC assessment help documents, Errata, and the Glossary/Acronyms document. Documents will open in a separate window.

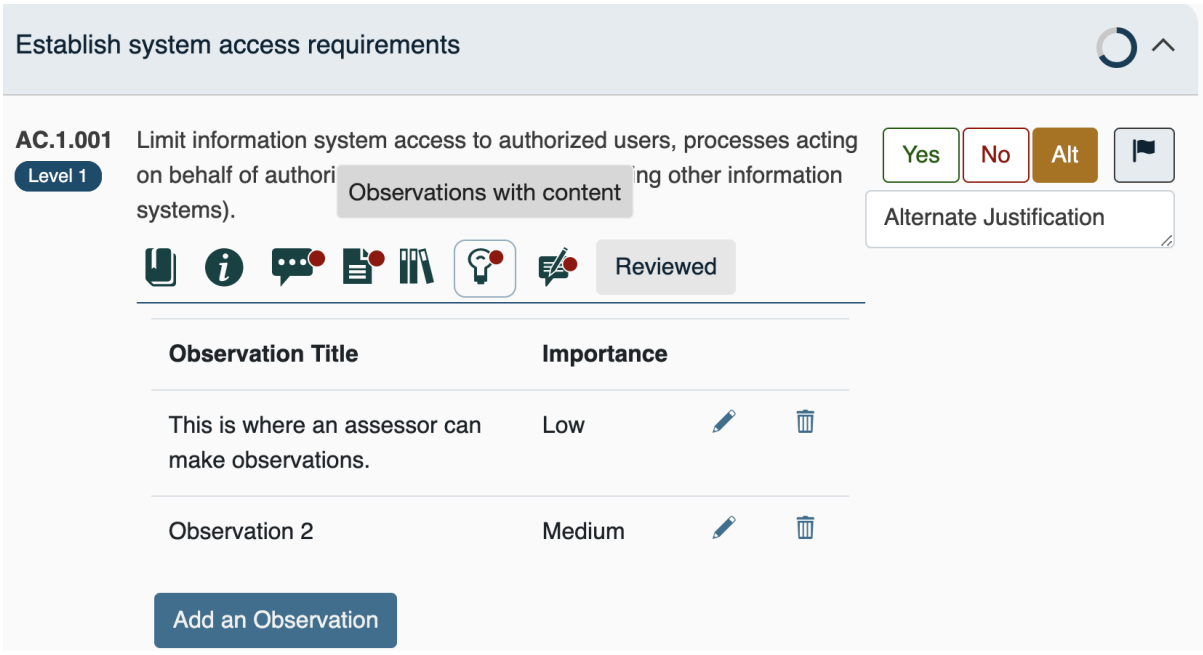


Observations

The Observations Icon opens a pop-up window that allows an assessor to record their observations for each practice question.

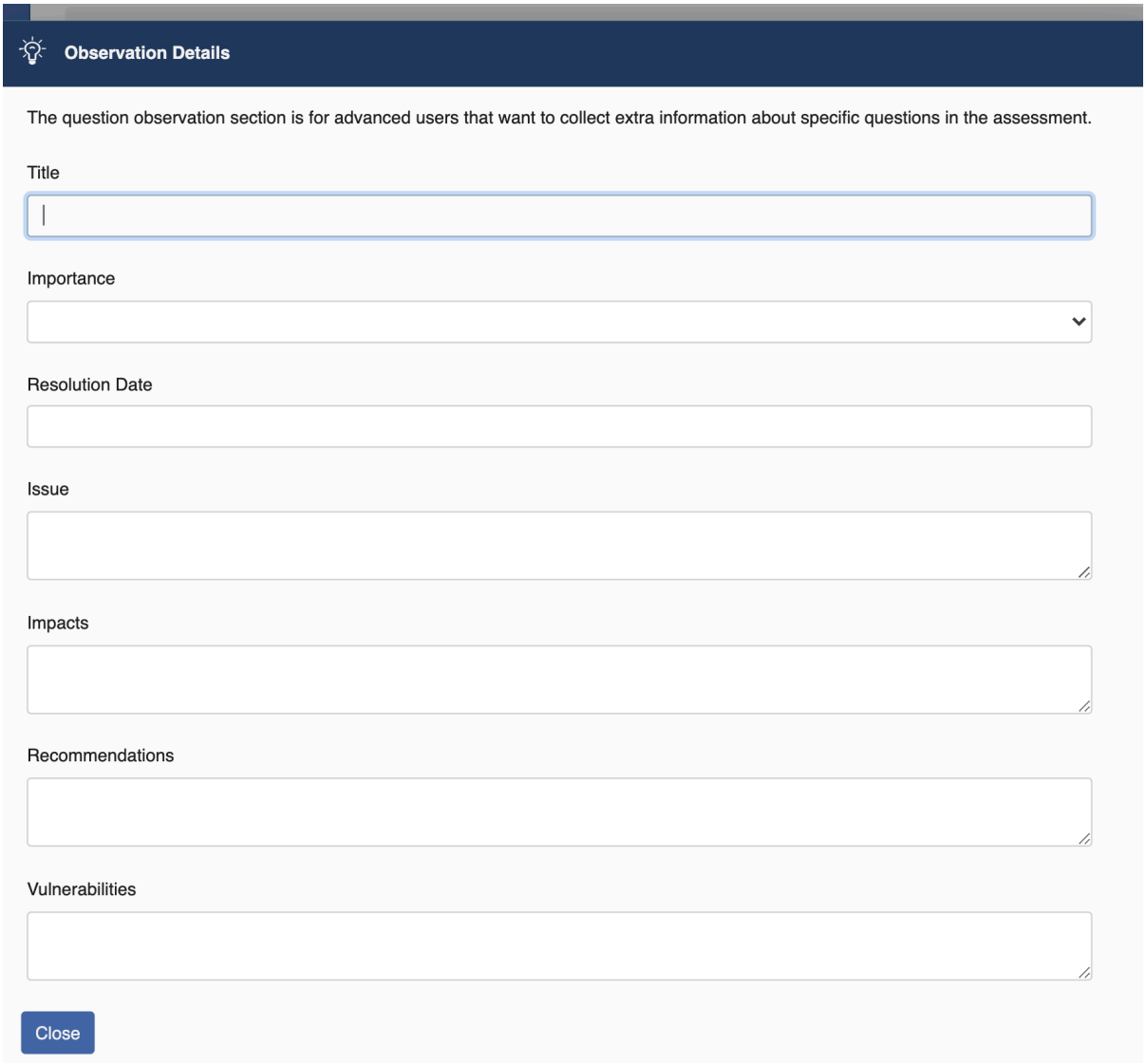


Once a user has entered their observations, a red indicator highlights the icon and the observations are listed beneath the practice question in order of entry.



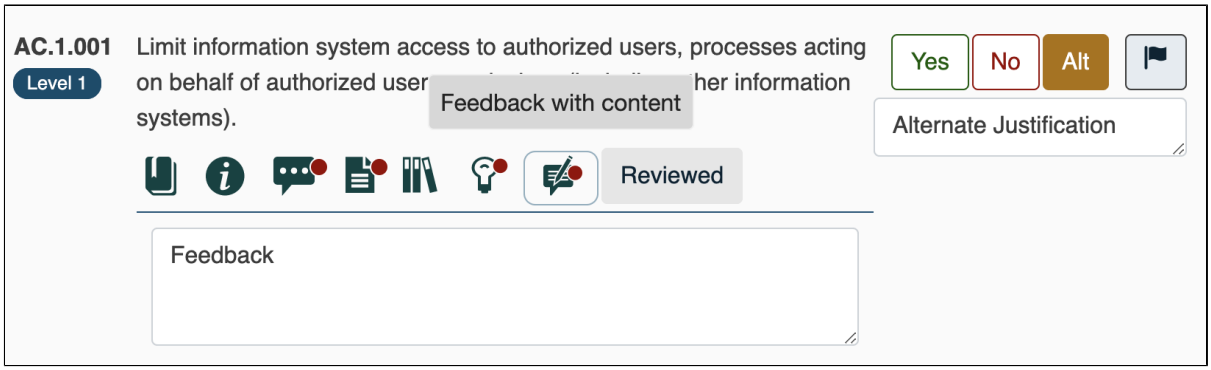
Observations Details Pop-Up Screen:

After selecting the Observations Icon, the Observations Details screen appears.



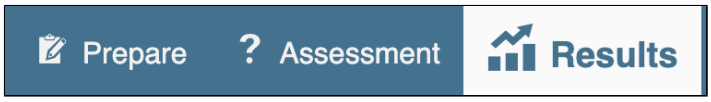
Feedback

Users can record Feedback during the assessment for submission to CSET/DHS. Some examples of submitted feedback include commentary on the subject matter of the question, the structure of the question, and how the question and layout can be improved.



5. CMMC Results

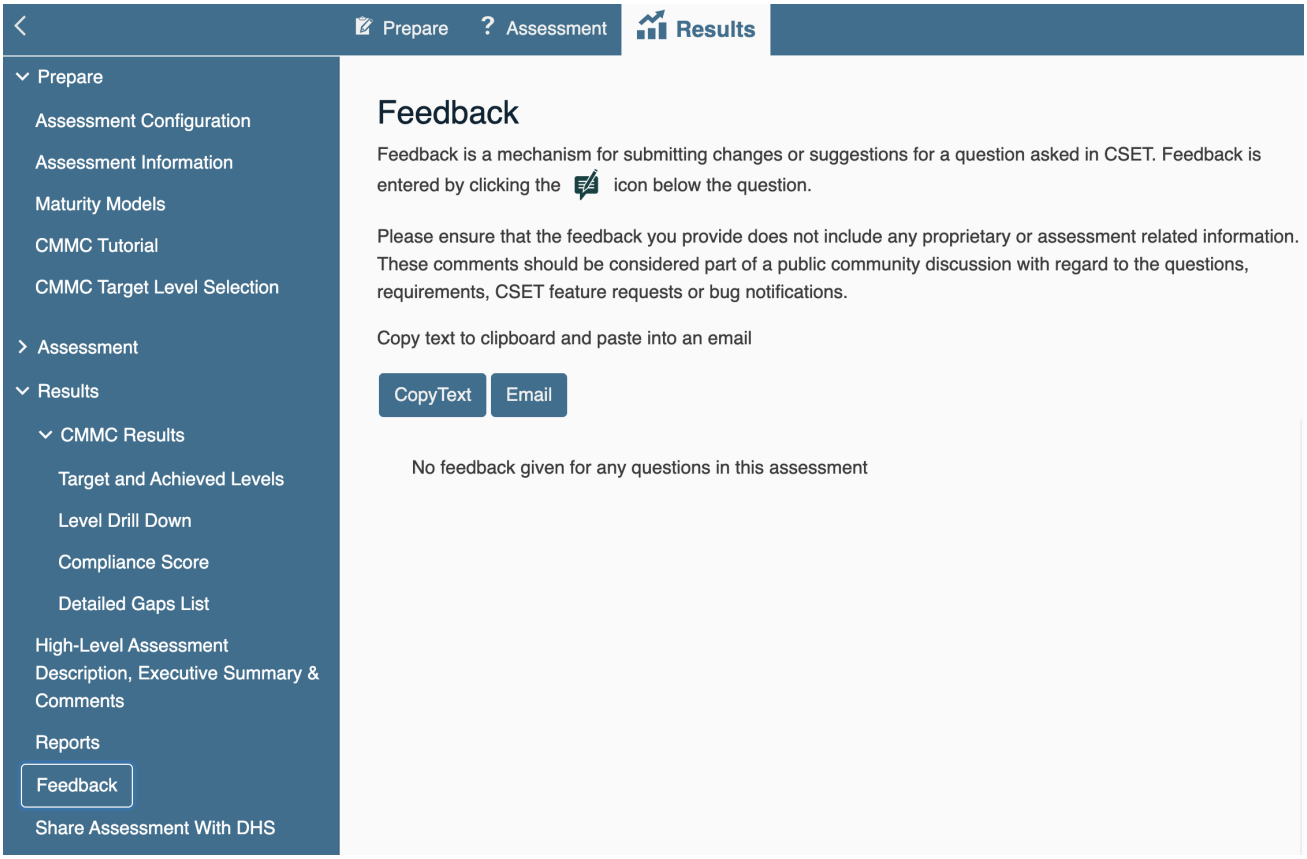
6. CMMC Reports



The primary deliverable of a CMMC assessment is the CMMC Site Report which contains the findings associated with the assessment. To learn more about the CMMC Results and Report functionality, visit the **Results** and **Reports** section of the CMMC User Guide.

7. Submit Feedback

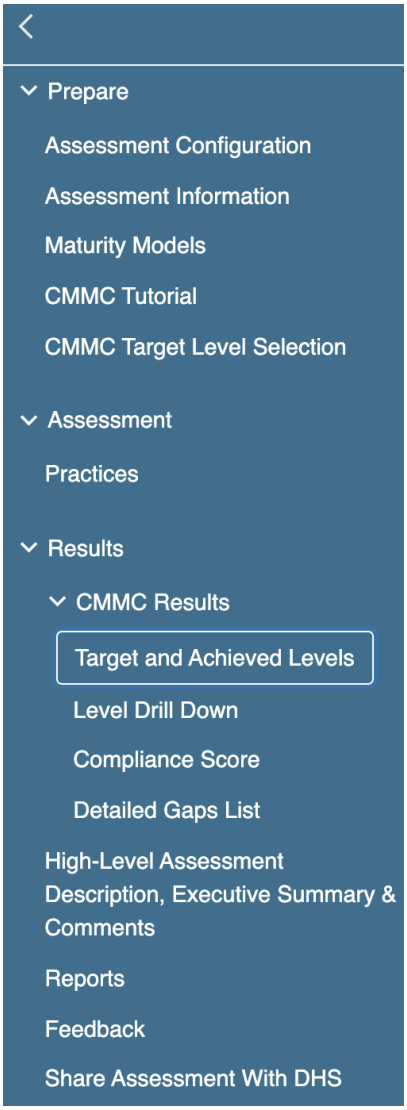
At the end of the assessment, users are prompted to submit their feedback on the CSET Assessment.



3.2. Results

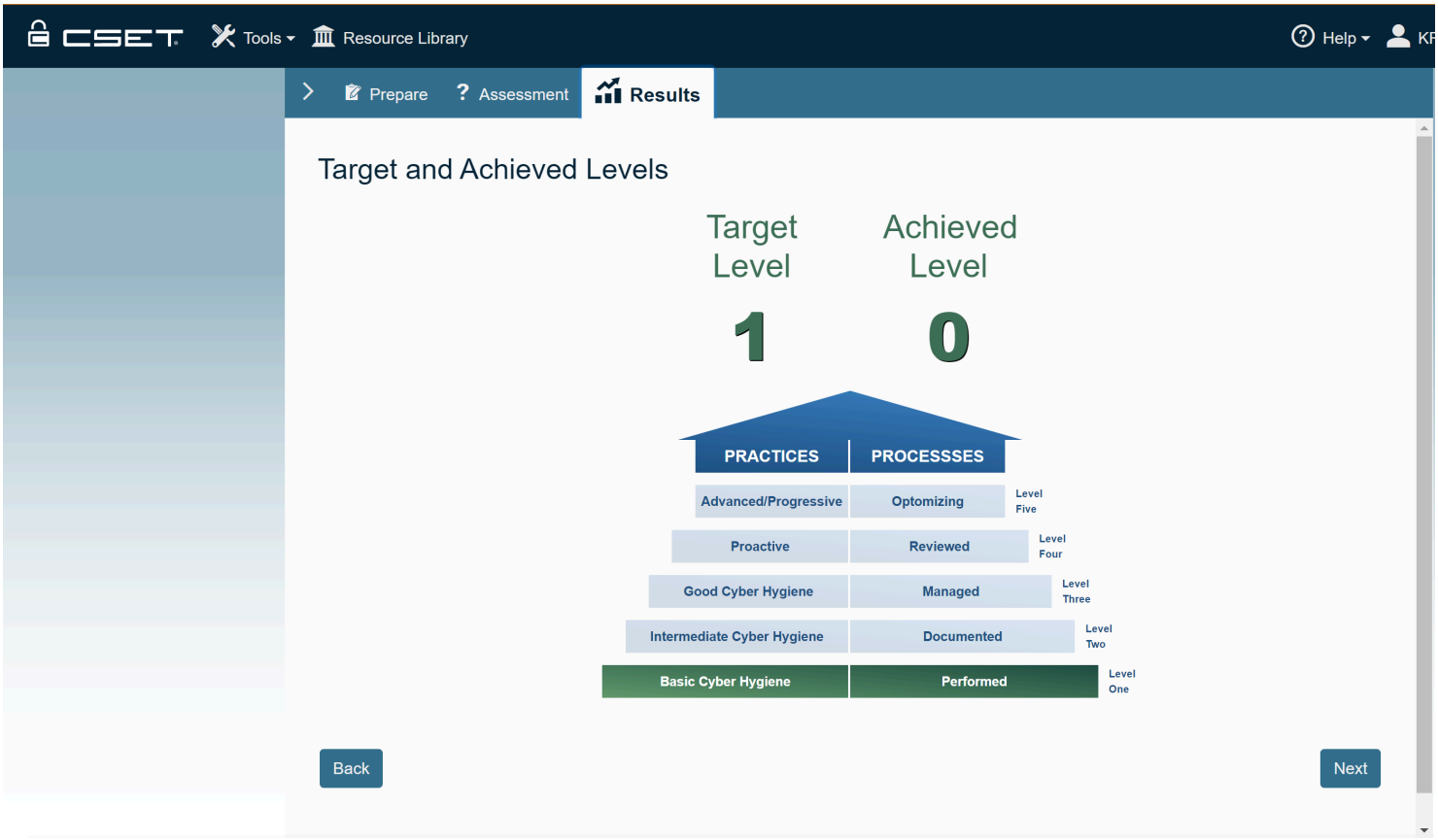
Results Tab

CMMC presents the Results of an assessment with the following sidebar navigation options:



Target Level vs. Achieved Level

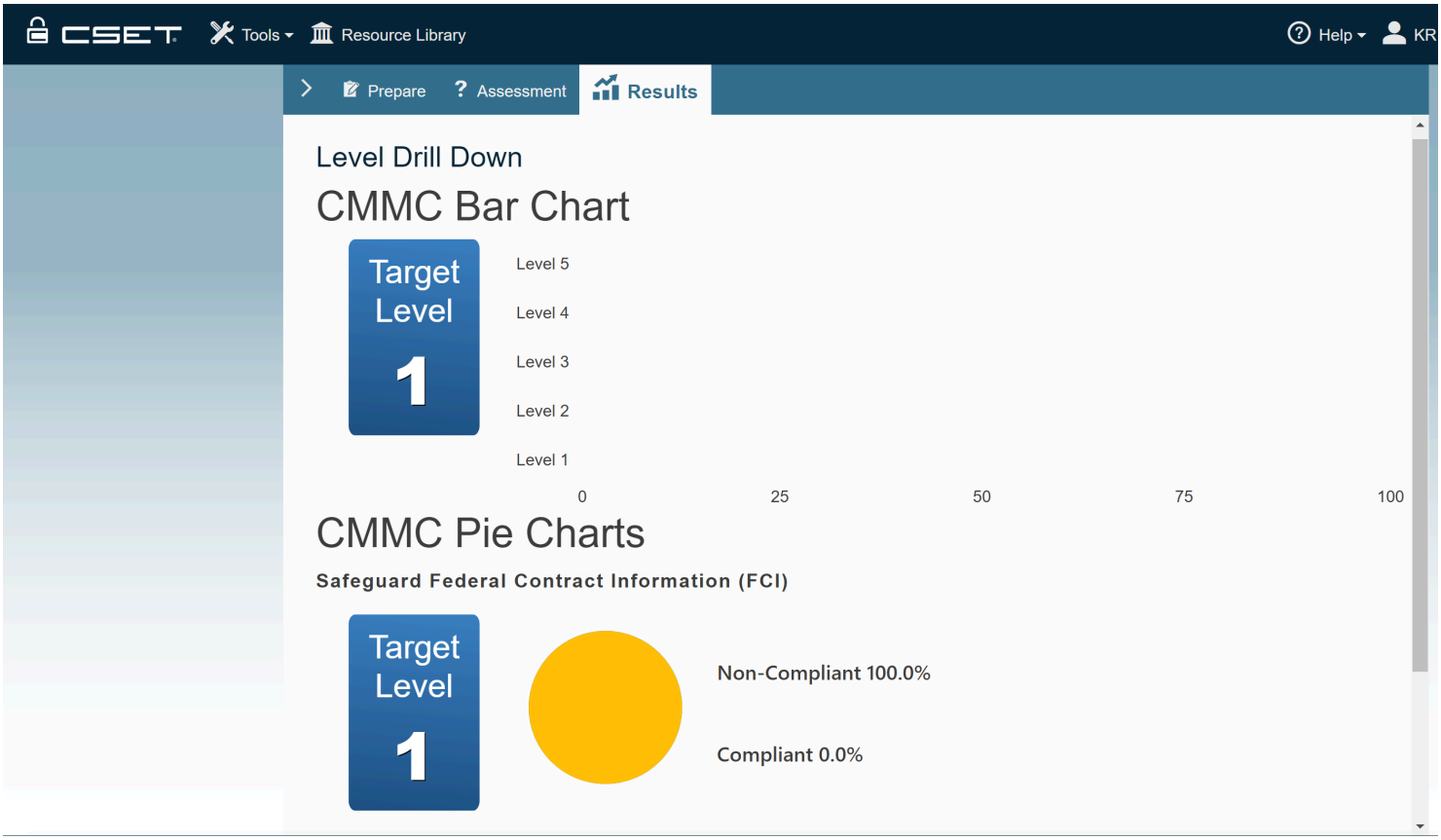
This graph displays the results for the current user-selected CMMC assessment target level vs. the CMMC level attained post-assessment.



Level Drill Down

CMMC Bar Chart: Details the percentage of compliance for each level assessed.

CMMC Pie Chart: Displays compliant vs. non-compliant percentages for each level assessed.

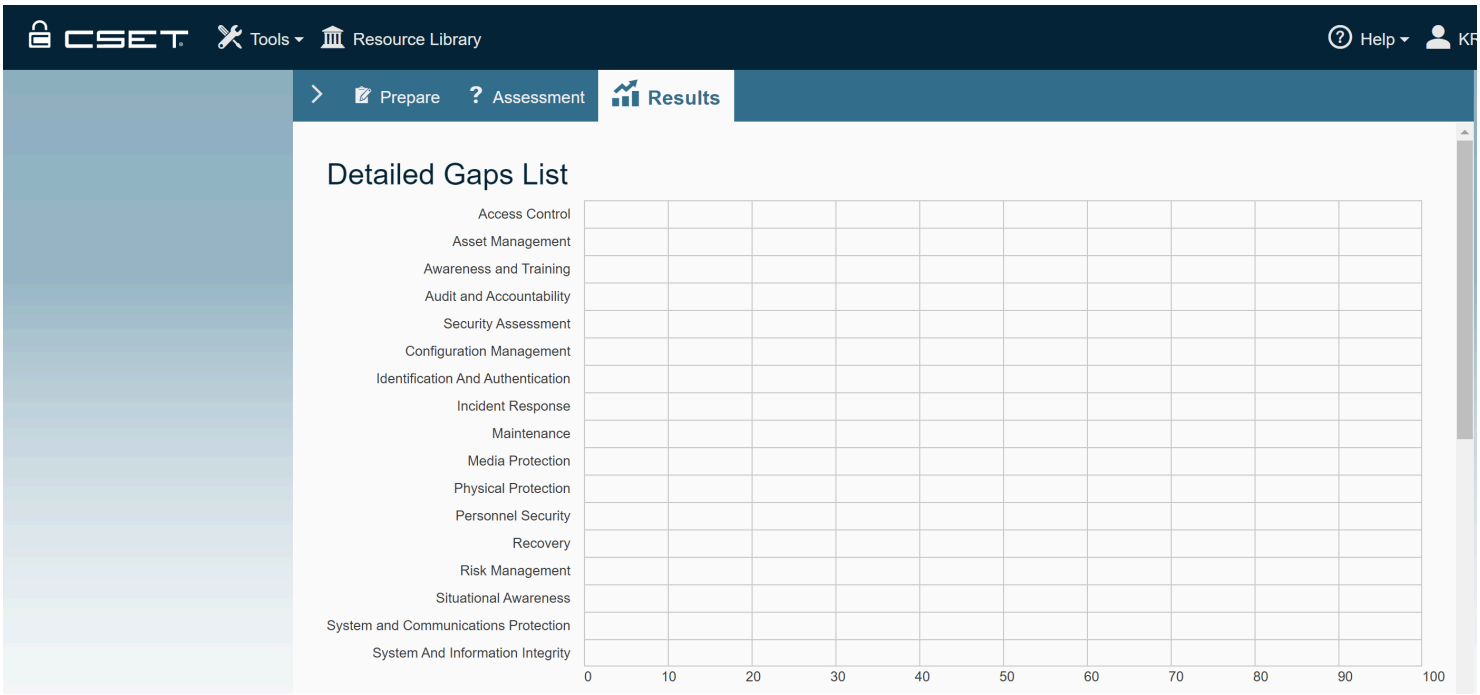


Compliance Score

This graph shows the total compliance score for the set target level broken down by total practices satisfied per level.

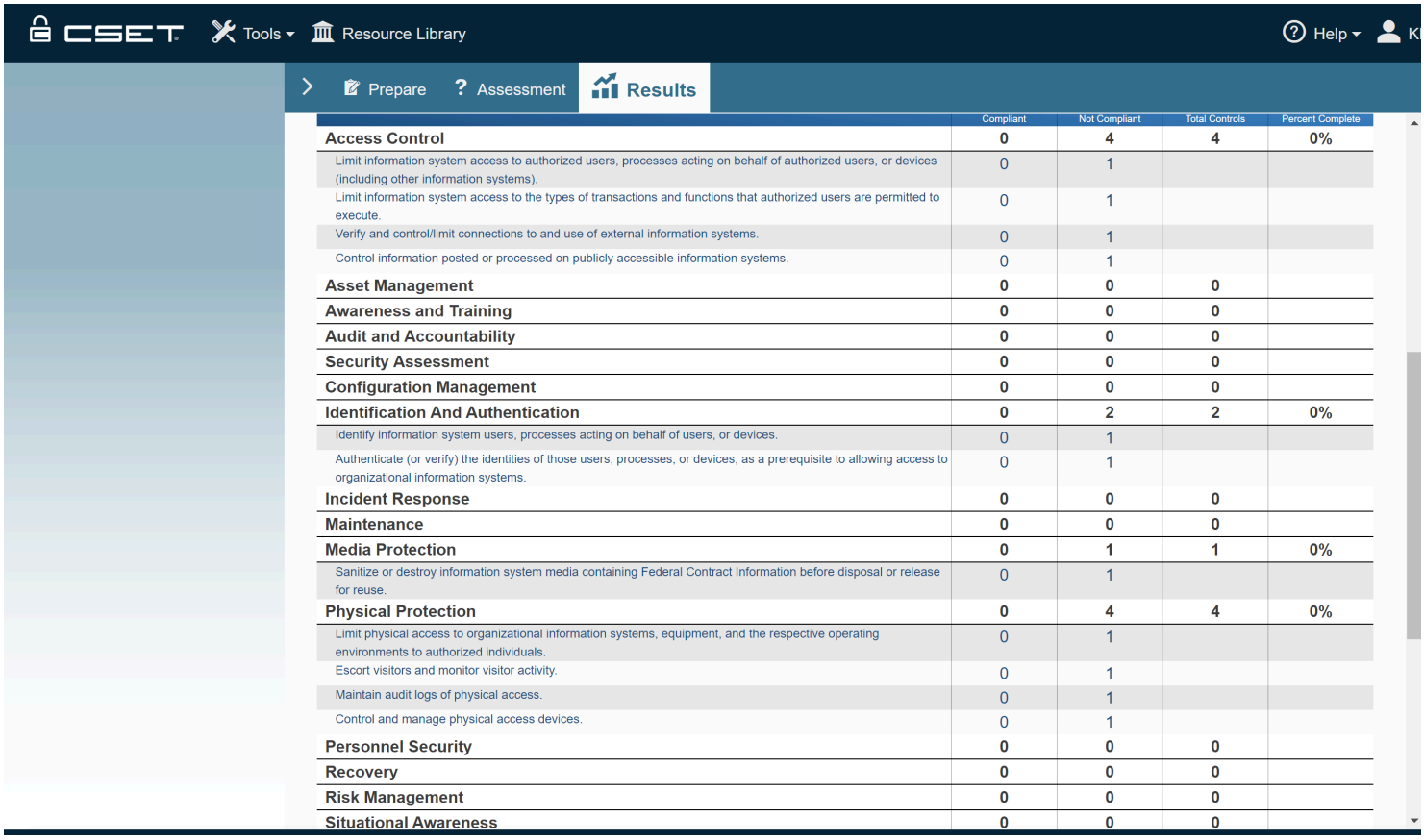
Detailed Gap Analysis

This section shows the gap analysis for each domain.



Gap Analysis Scorecard

This section shows each CMMC domain with the individual practices detailed in list format after each domain-specific sub heading. The compliance score for each individual practice is shown on the right, along with the associated cumulative score for each practice and the percent complete for each CMMC domain.

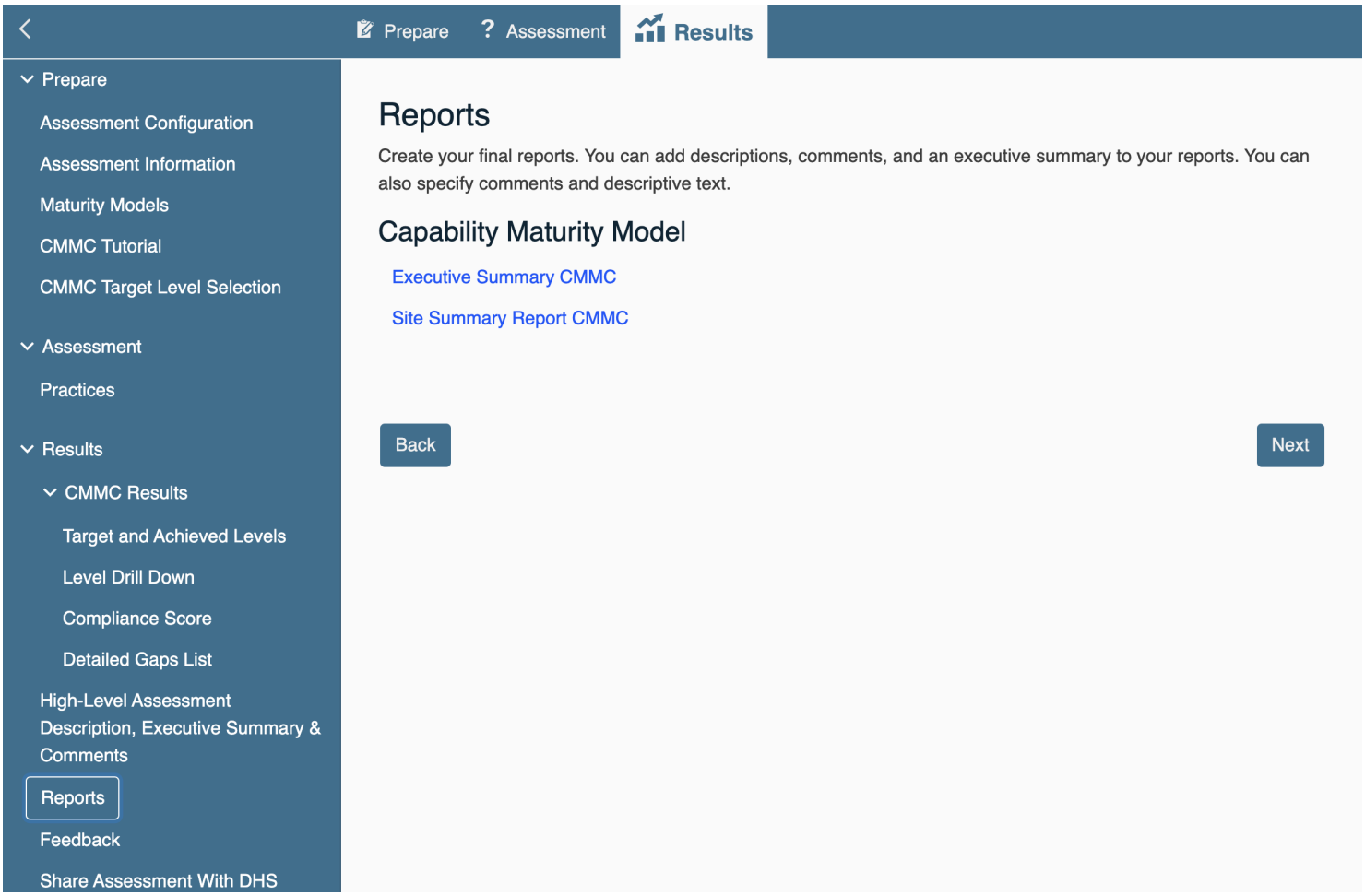


	Compliant	Not Compliant	Total Controls	Percent Complete
Access Control	**0**	**4**	**4**	**0%**
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	0	1		
Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	0	1		
Verify and control/limit connections to and use of external information systems.	0	1		
Control information posted or processed on publicly accessible information systems.	0	1		
Asset Management	**0**	**0**	**0**	
Awareness and Training	**0**	**0**	**0**	
Audit and Accountability	**0**	**0**	**0**	
Security Assessment	**0**	**0**	**0**	
Configuration Management	**0**	**0**	**0**	
Identification And Authentication	**0**	**2**	**2**	**0%**
Identify information system users, processes acting on behalf of users, or devices.	0	1		
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	0	1		
Incident Response	**0**	**0**	**0**	
Maintenance	**0**	**0**	**0**	
Media Protection	**0**	**1**	**1**	**0%**
Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	0	1		
Physical Protection	**0**	**4**	**4**	**0%**
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	0	1		
Escort visitors and monitor visitor activity.	0	1		
Maintain audit logs of physical access.	0	1		
Control and manage physical access devices.	0	1		
Personnel Security	**0**	**0**	**0**	
Recovery	**0**	**0**	**0**	
Risk Management	**0**	**0**	**0**	
Situational Awareness	**0**	**0**	**0**	

7.3. Reports

Reports

This section includes the **Executive Summary Report** and **Site Summary Report** specific to CMMC.



The Executive Summary Report Includes:

1. Assessment Target Level - CMMC Practices and Processes
2. CMMC Compliance by Domain
3. Compliance Score Breakdown

The Site Summary Report Includes:

1. Site Information
2. Assessment Target Level - CMMC Practices and Processes
3. CMMC Processes and Practices Explained
4. High-Level Assessment Description
5. Compliance Score Breakdown
6. CMMC Compliance by Domain
7. CMMC Requirements Scoring
8. CMMC Statements Gap List with Corresponding References

E X E C U T I V E S U M M A R Y C M M C

S I T E S U M M A R Y R E P O R T C M M C