PRE-ASSESSMENT WEBFORMS

Instructions for the Completion and Review of the Pre-Assessment Webforms

v.HT-2112-01

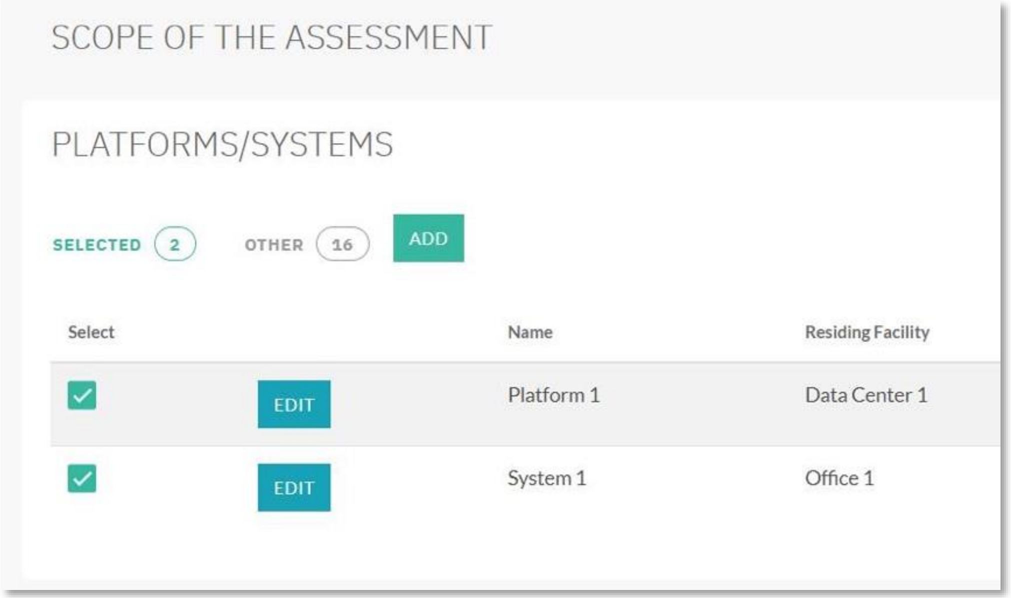
HITRUST®

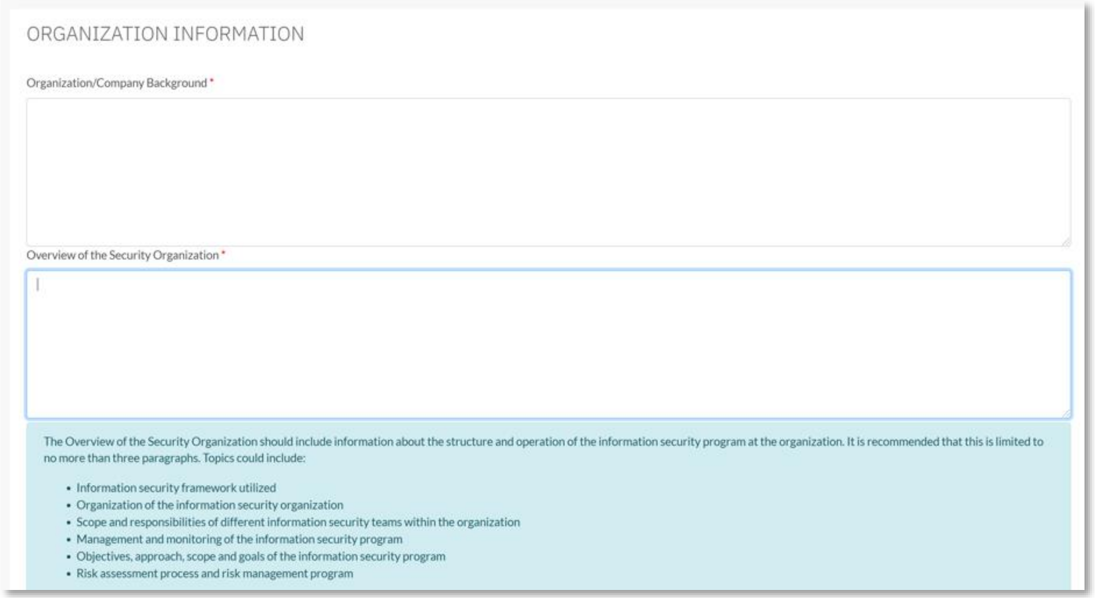
Table of Contents

ORGANIZATION INFORMATION AND SCOPE OF THE ASSESSMENT WEBFORMS

Summary: Organization Information and Scope of the Assessment Webforms

- Integrated into MyCSF and streamlined to reduce redundancy and enhance clarity of what is in scope
- Addition of automated checks and tool tips to avoid common scoping issues
- Streamlined presentation of scope in a tabular format inclusive of both platforms and facilities in scope
- Easier identification of third-party service providers



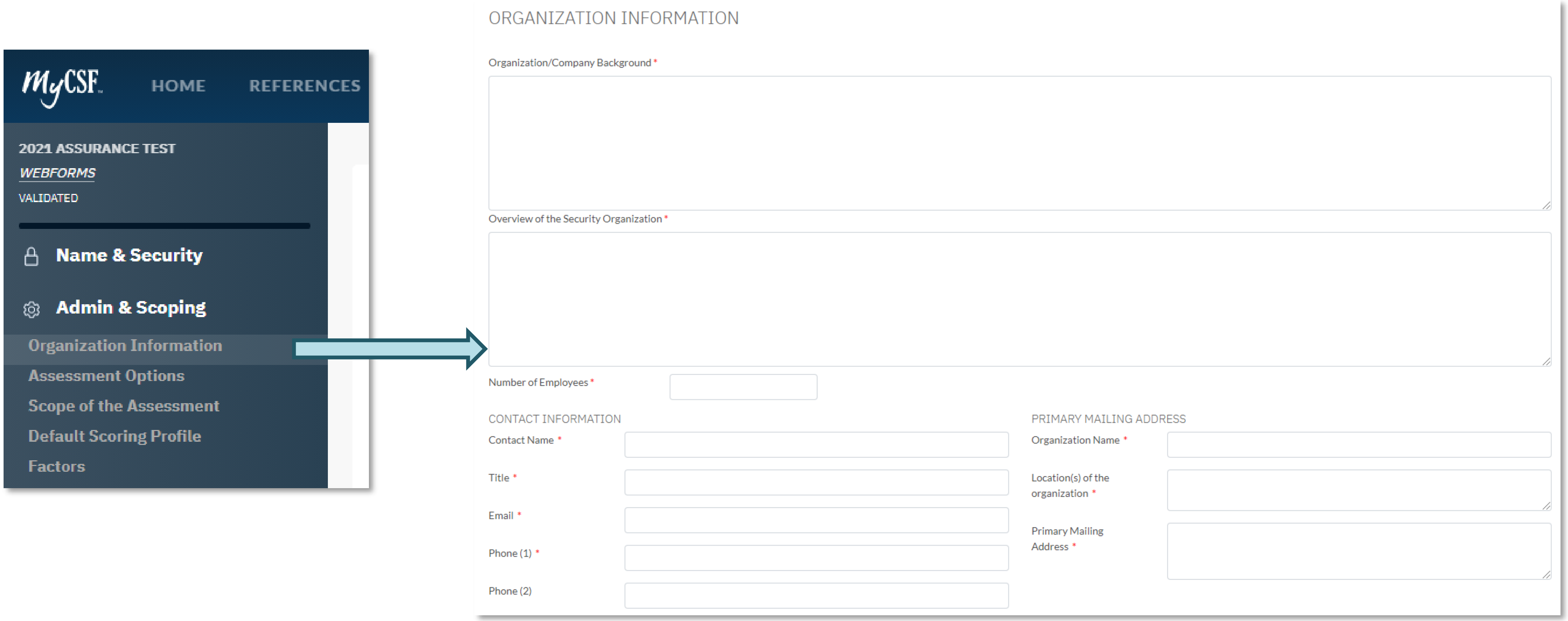


HOW TO COMPLETE THE ORGANIZATION INFORMATION WEBFORM

Assessed Entity Instructions

Instructions: How to Complete the Organization Information Webform

Step 1 - The Assessed Entity should access the assessment in MyCSF and, within the assessment object, navigate to the Organization Information webform by clicking *Organization Information* on the left sidebar.



Instructions: How to Complete the Organization Information Webform

Step 2 - The Assessed Entity should complete the Organization/Company Background section following the guidelines presented within the tool.

Note: *This section replaces the Organization and Industry Segment Overview from the offline Organizational Overview and Scope document that is no longer utilized. <u>This section will appear in the final report. Please review for spelling and grammar issues and ensure that the formatting is as you would like it to appear in the report.</u>*

Organization/Company Background *

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

The Company Background section should be a one to two paragraph overview of your organization as a whole which will appear in the final report. Content could include your mission statement, values, or primary business lines. Content could be similar to the "About us" section of your website.

Do's and Do not's

- Do's:
  - Limit yourself to one to two paragraphs
  - Review your content for spelling and grammar issues
  - Give the reader an overview of what your organization does
- Do Not's:
  - Include information related to number of employees, geographic areas served, compliance requirements, or systems in scope as this information is presented elsewhere in the report
  - Use industry specific terms or acronyms that are not defined
  - Discuss scope of the assessment
  - Include marketing language such as "We are the best service provider..."

Instructions: How to Complete the Organization Information Webform

Step 3 - The Assessed Entity should complete the Overview of the Security Organization section following the guidelines presented within the tool.

__Note:__ This section replaces the Overview of the Security Organization from the offline Organizational Overview and Scope document that is no longer utilized. This section will appear in the final report. Please review for spelling and grammar issues and ensure that the formatting is as you would like it to appear in the report.

Overview of the Security Organization *

Chinstrap's information security function is housed under the larger information technology department. The information security function is led by the CISO who reports to the CIO. The information security function has developed a robust information security program focused on managing information security risk. Key elements of the program include:
- Risk management
- Network security
- Application security
- Physical security
- Business continuity and disaster recovery

The Overview of the Security Organization should include information about the structure and operation of the information security program at the organization. It is recommended that this is limited to no more than three paragraphs. Topics could include:

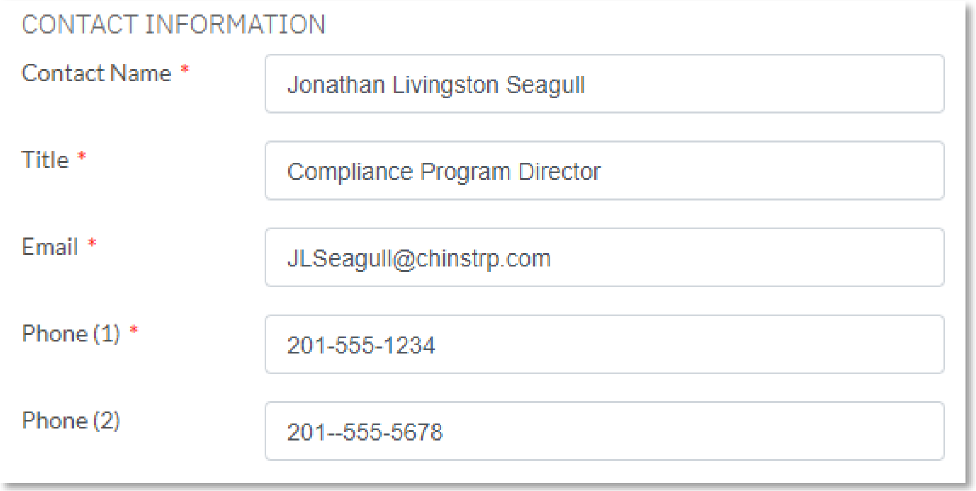
- Information security framework utilized
- Organization of the information security organization
- Scope and responsibilities of different information security teams within the organization
- Management and monitoring of the information security program
- Objectives, approach, scope and goals of the information security program
- Risk assessment process and risk management program

Do's and Do not's

- Do's:
  - Utilize spelling and grammar checking tools
  - Be concise and limit your content to information that a reader of the report would be interested in knowing
  - Keep your content high level
- Do Not's:
  - Discuss specific tools
  - Include information about the scope of the assessment
  - Include information that is considered confidential to your organization

Instructions: How to Complete the Organization Information Webform

Step 4 – Complete the Contact Information section including Contact Name, Title, Email, and Phone Number


CONTACT INFORMATION

Contact Name * Jonathan Livingston Seagull

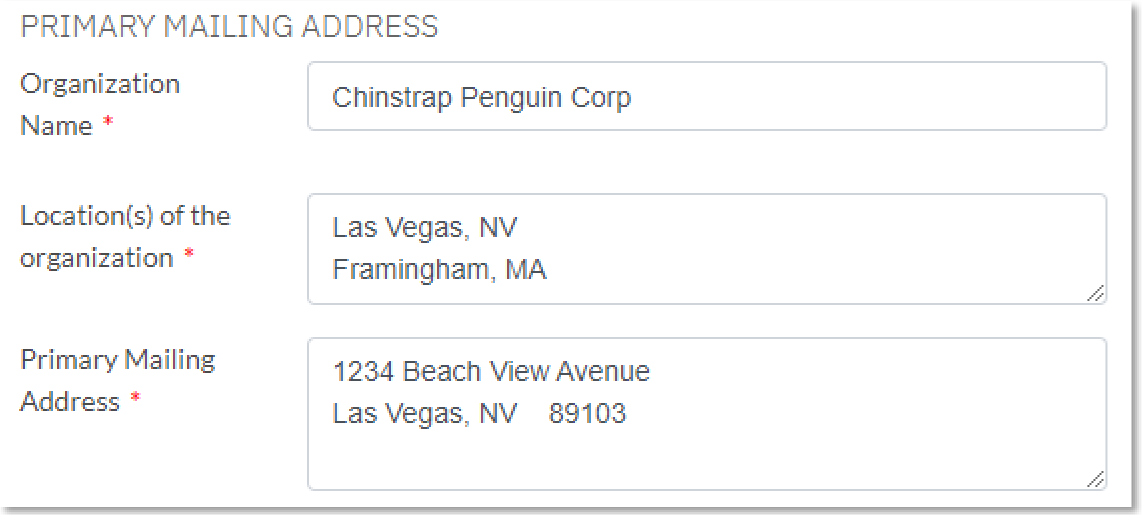
Title * Compliance Program Director

Email * JLSeagull@chinstrp.com

Phone (1) * 201-555-1234

Phone (2) 201--555-5678

Step 5 – Complete the Primary Mailing Address Section including the Organization Name, Location(s) of the Organization, and Primary Mailing Address


PRIMARY MAILING ADDRESS

Organization Name * Chinstrap Penguin Corp

Location(s) of the organization * Las Vegas, NV
Framingham, MA

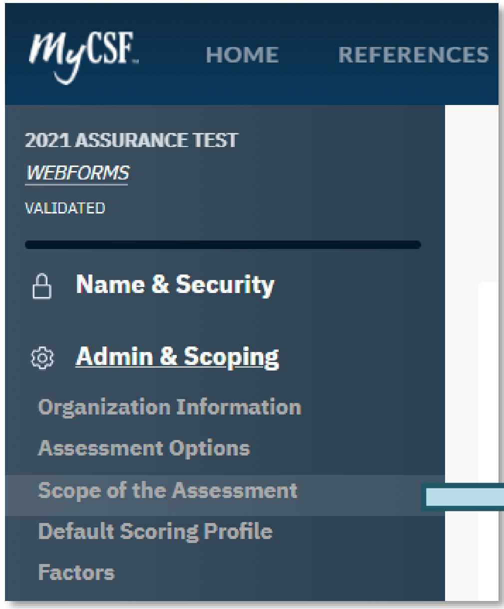
Primary Mailing Address * 1234 Beach View Avenue
Las Vegas, NV 89103

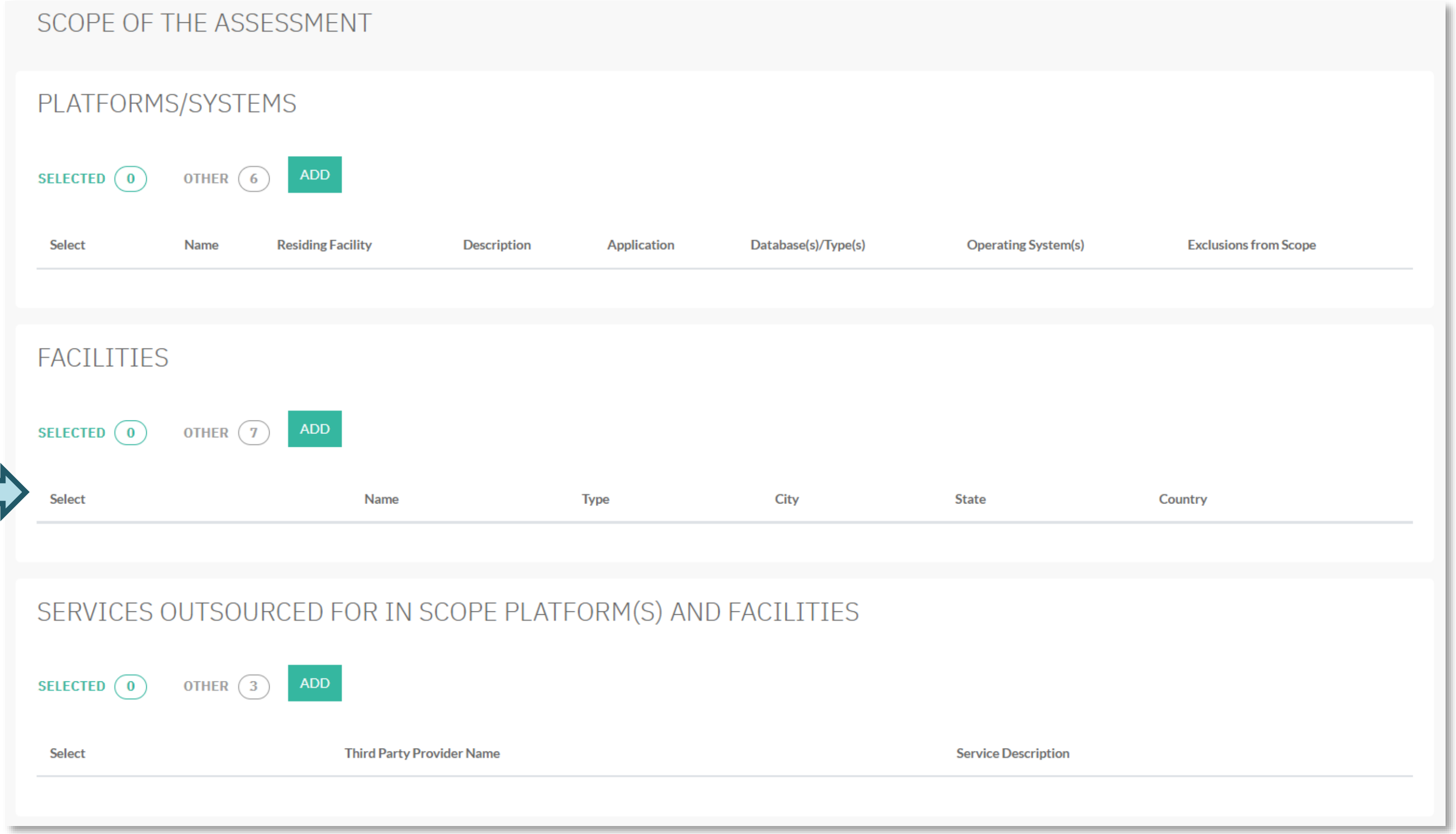
HOW TO COMPLETE THE SCOPE OF THE ASSESSMENT WEBFORM

Assessed Entity Instructions

Instructions: How to Complete the Scope of the Assessment Webform

Step 1 - The Assessed Entity should access the assessment in MyCSF and, within the assessment object, navigate to the Scope of the Assessment webform by clicking *Scope of the Assessment* on the left sidebar.



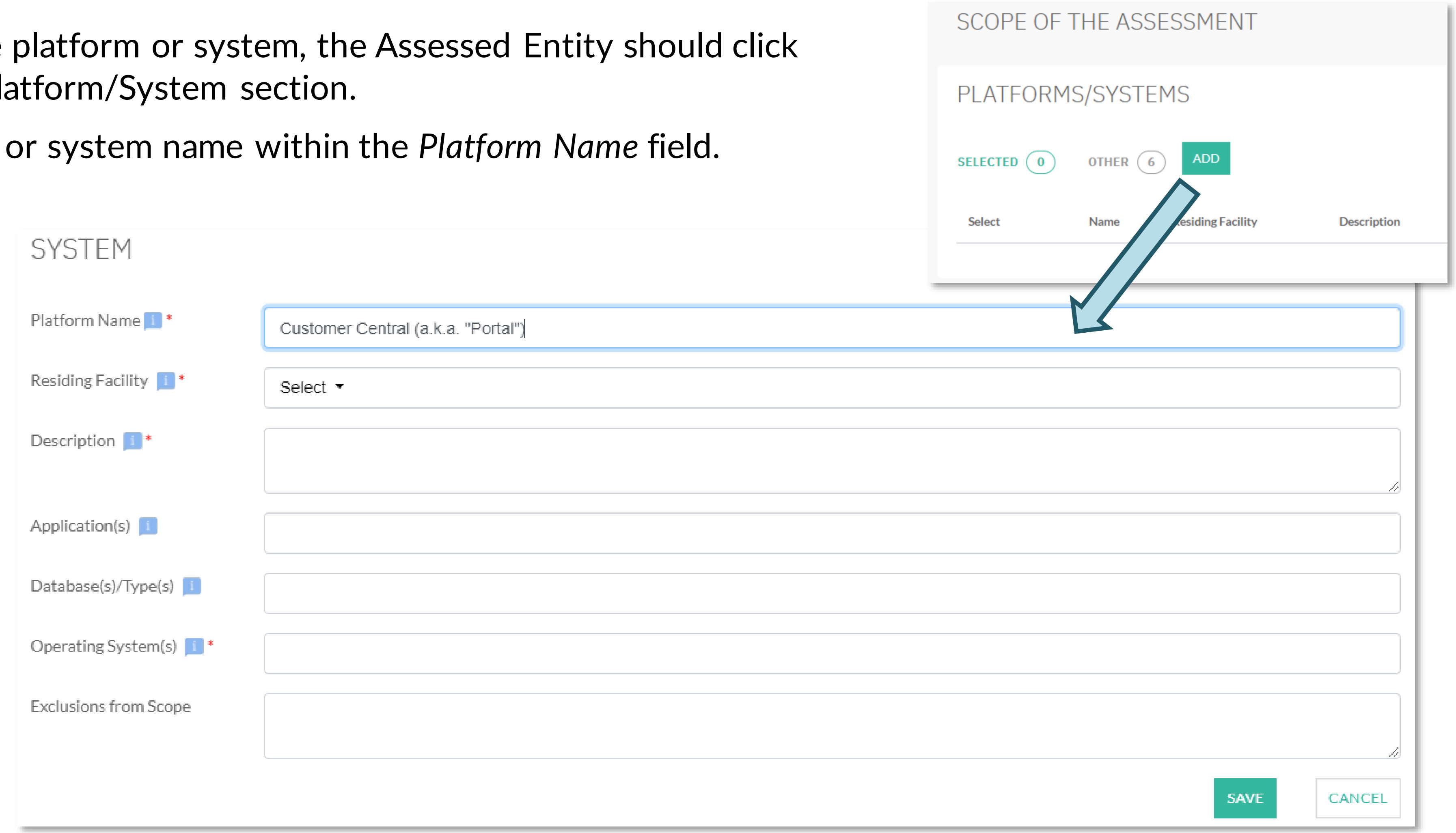


Note: *The Platforms/Systems, Facilities, and Services Outsourced entered within this webform will appear in the scoping section of the final report.*

Instructions: How to Complete the Scope of the Assessment Webform

Step 2a – To add an in-scope platform or system, the Assessed Entity should click the *ADD* button within the Platform/System section.

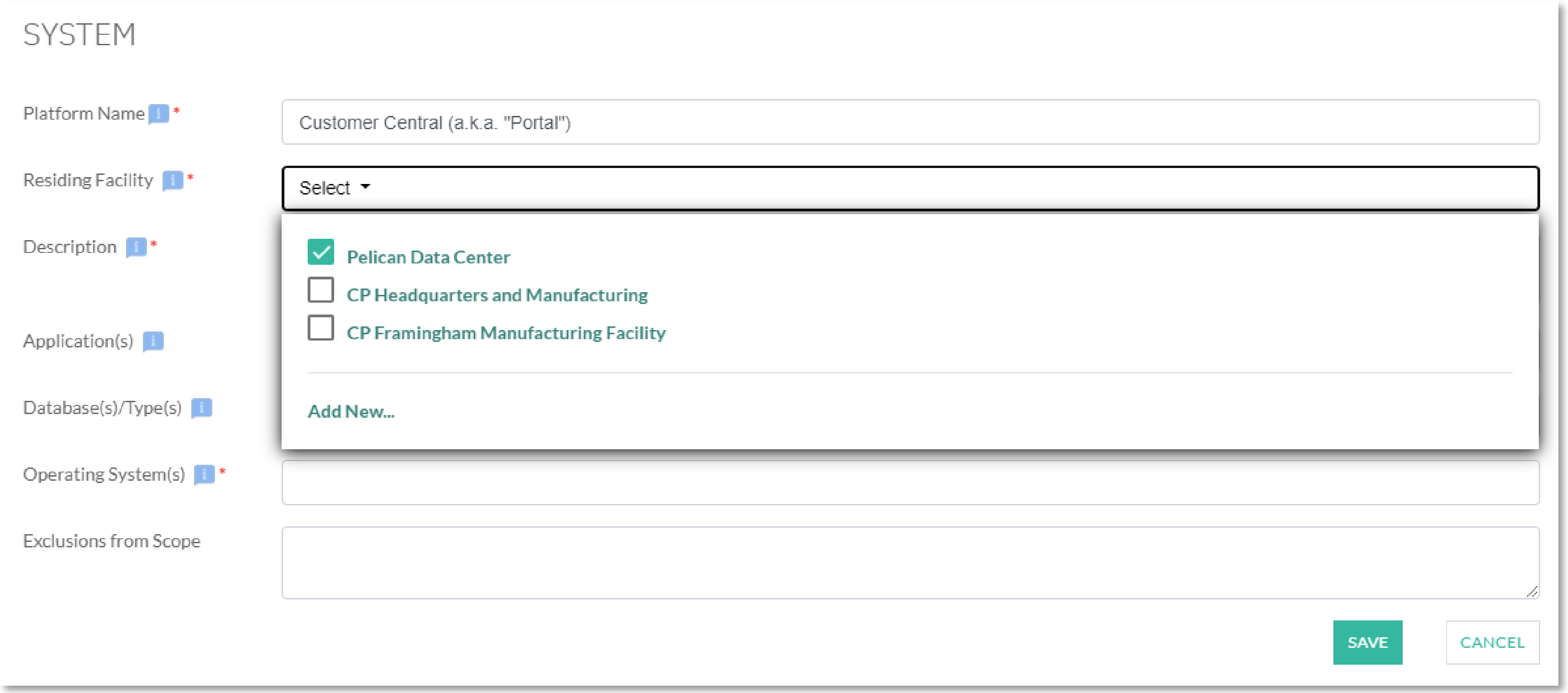
Step 2b – Enter the platform or system name within the *Platform Name* field.



Instructions: How to Complete the Scope of the Assessment Webform

Step 2c – Select the residing facility for the platform from the list of any facilities that have already been entered into the tool or click *Add New* if the residing facility has not yet been added.

Note: *If you have clicked "Add New" skip to step 3b to view instructions for adding a facility. After the facility has been added, return to step 2c and select the facility from the list.*



Instructions: How to Complete the Scope of the Assessment Webform

Step 2d – Enter a description of the platform or system. The description should include relevant technical details around the platform (describing any exclusions), a description of the scope boundary (including any supporting infrastructure), and how the platform is accessed by the organization, the organization's customers, and third-parties, if applicable.

SYSTEM

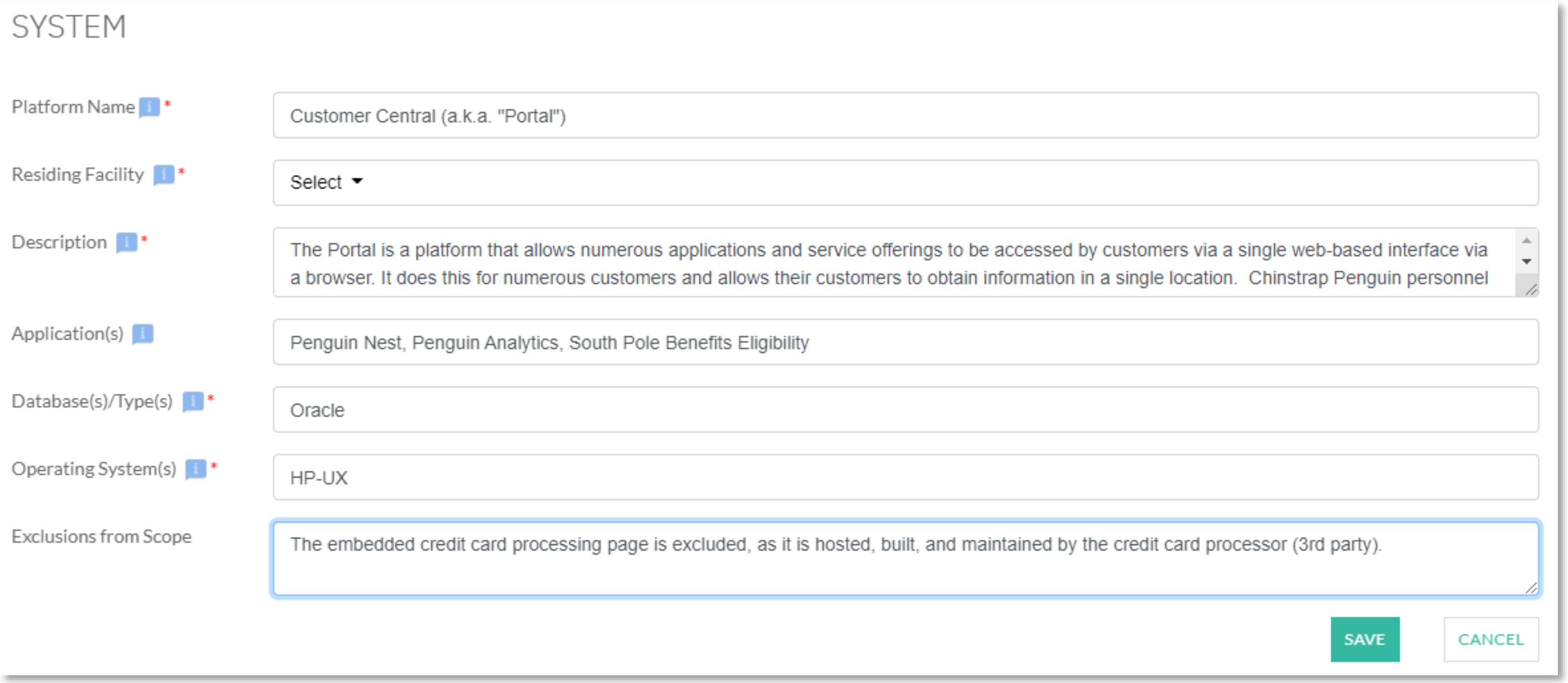
Platform Name *	Customer Central (a.k.a. "Portal")
Residing Facility *	Select
Description *	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. - Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. - Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. - South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.
Application(s)	

Instructions: How to Complete the Scope of the Assessment Webform

Step 2e – Enter any applications, databases, and operating systems for the platform.

Note: *The Database(s)/Type(s) field is required to be filled out when an Application has been included. The Operating System(s) field is required to be filled out when either an application or database has been included.*

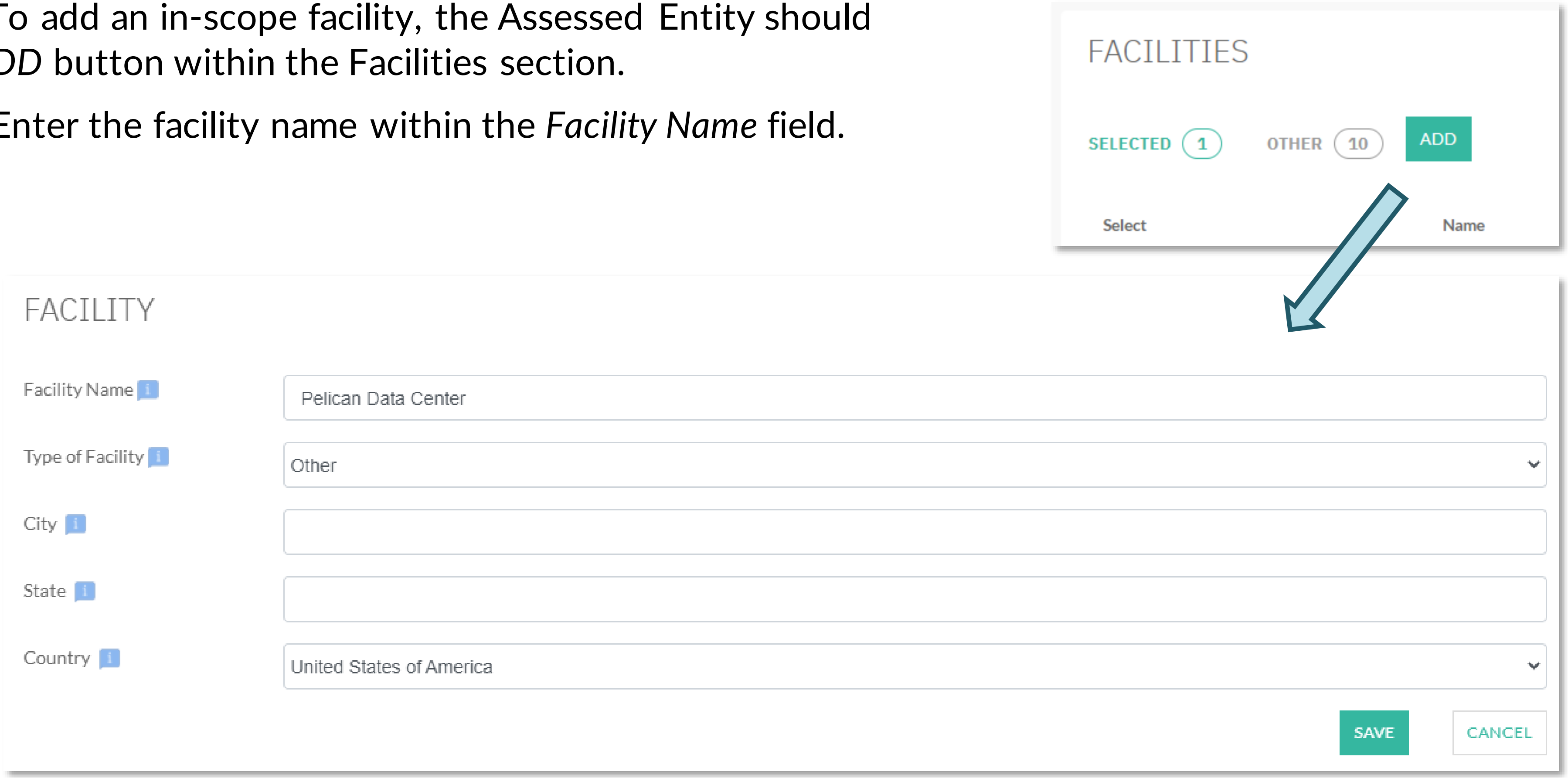
Step 2f – Enter any exclusions from scope related to this platform.



Instructions: How to Complete the Scope of the Assessment Webform

Step 3a – To add an in-scope facility, the Assessed Entity should click the *ADD* button within the Facilities section.

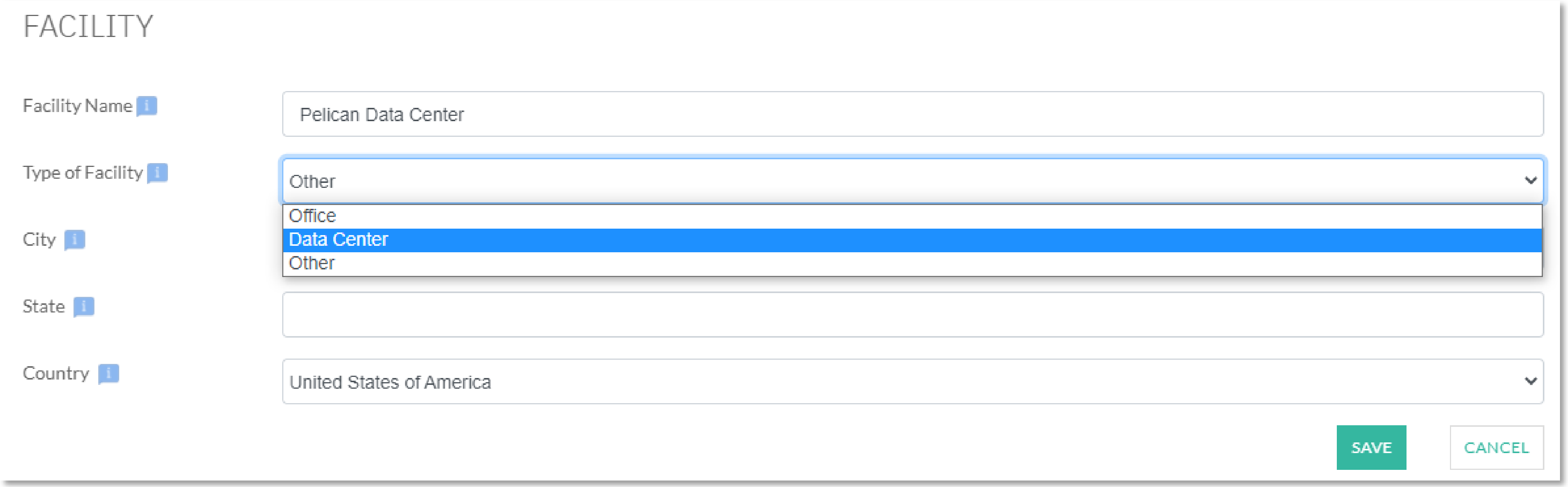
Step 3b – Enter the facility name within the *Facility Name* field.



Instructions: How to Complete the Scope of the Assessment Webform

Step 3c – Select the type of facility from the drop-down list.

Note: *If you selected Office or Other, you may skip steps 3d and 3e.*

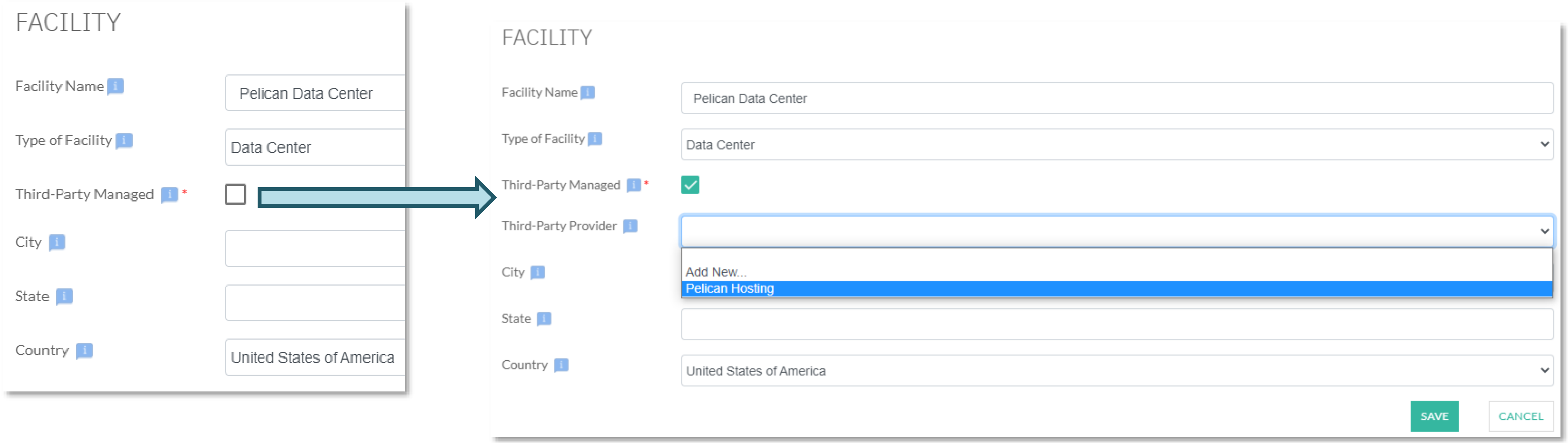


Instructions: How to Complete the Scope of the Assessment Webform

Step 3d – If the type of facility selected is Data Center, the Assessed Entity should indicate whether the data center is managed by a third-party to the Assessed Entity.

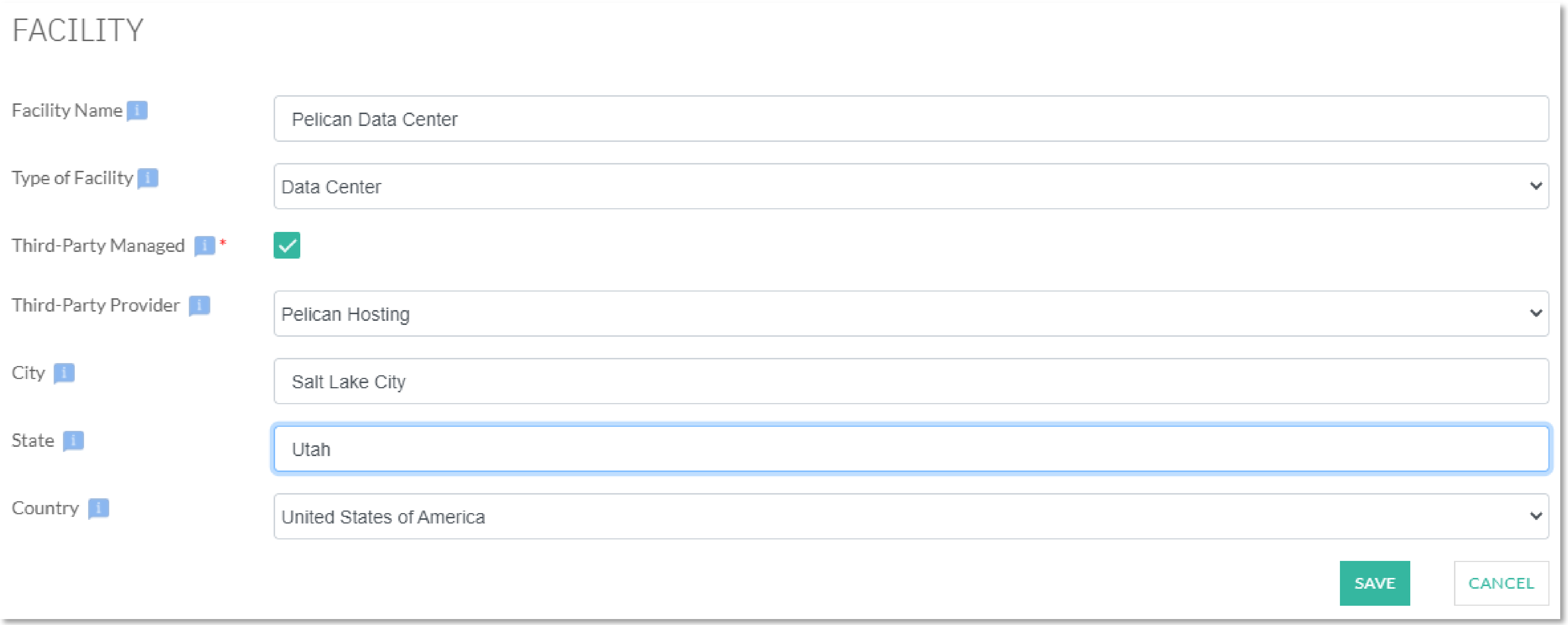
Step 3e – If the data center is managed by a third party, select the third party from the list of any third parties that have already been entered into the tool or click *Add New…* if the third party has not yet been added.

***Note:** If you clicked "Add New…", skip to step 4b to view instructions for adding a third-party provider to the Services Outsourced for In Scope Platforms and Facilities table. After the third party has been added, return to step 3e and select the third party from the list.*



Instructions: How to Complete the Scope of the Assessment Webform

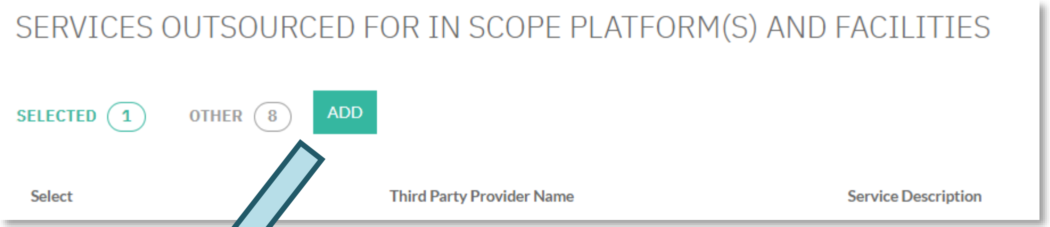
Step 3f – Enter the city, state, and country where the facility is located.

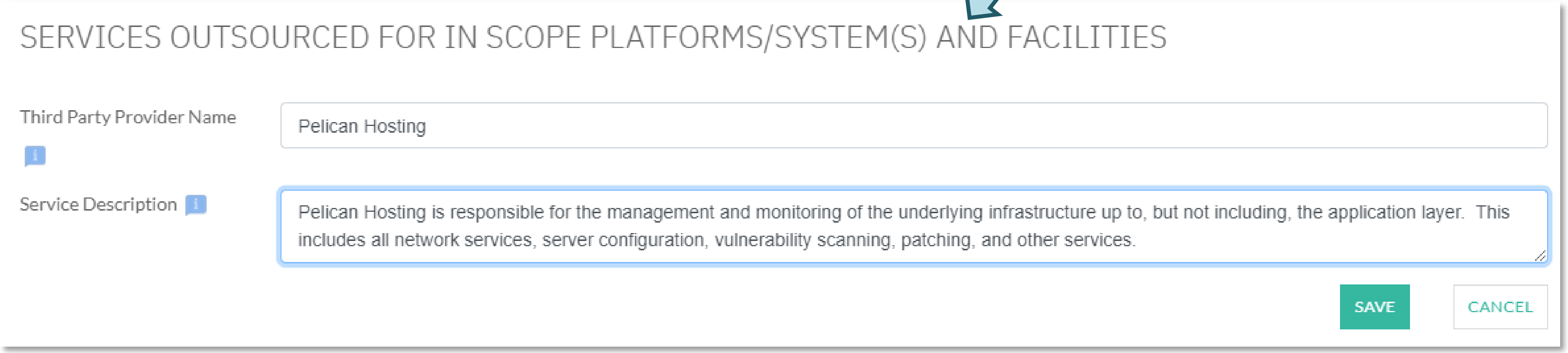


Instructions: How to Complete the Scope of the Assessment Webform

Step 4a – To add a third-party provider, the Assessed Entity should click the *ADD* button within the Services Outsourced for In Scope Platforms/Systems and Facilities section.

Step 4b – Enter the third-party provider's name and a description of the services provided by the third party relevant to the in-scope platforms and facilities.





***Note:** Only outsourced services that impact the controls for an in scope platform should be included within this table.*

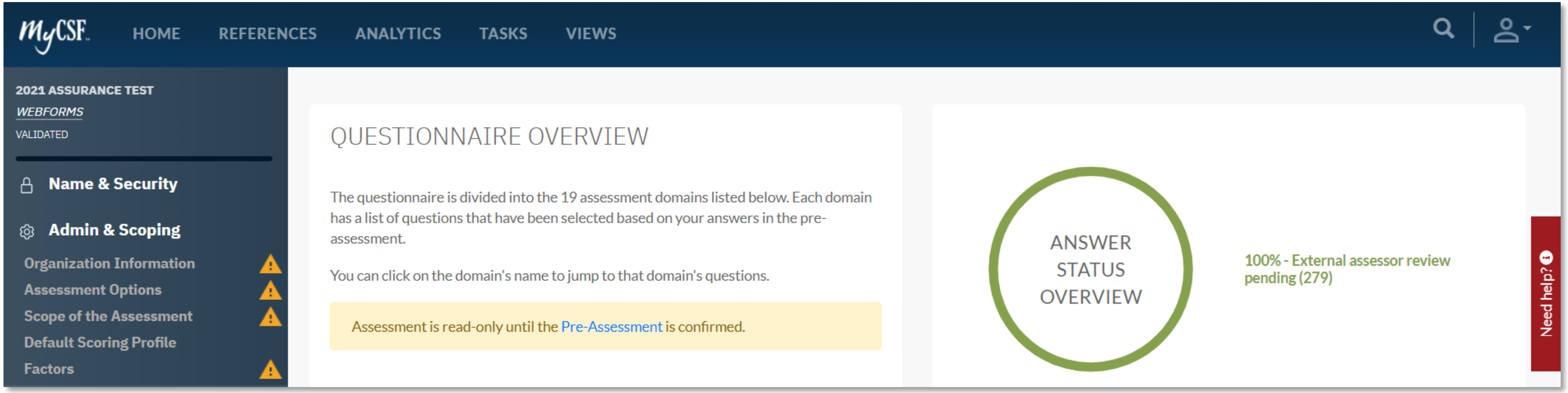
HOW TO REVIEW THE PRE-ASSESSMENT WEBFORMS

External Assessor Instructions

Reviewing the Pre-Assessment

The External Assessor must review the Pre-Assessment webforms prior to validating requirement statement scoring in order to ensure that:

- The organization and scoping information entered by the Assessed Entity is ready to be included in the final report.
- The External Assessor understands the scope of the assessment.
- The factor responses appropriately represent the scoped environment.

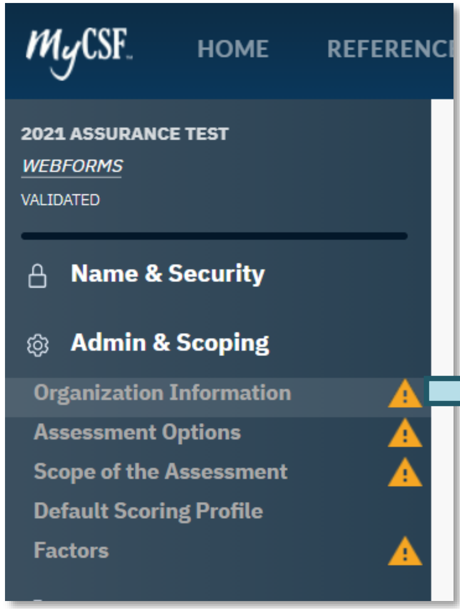


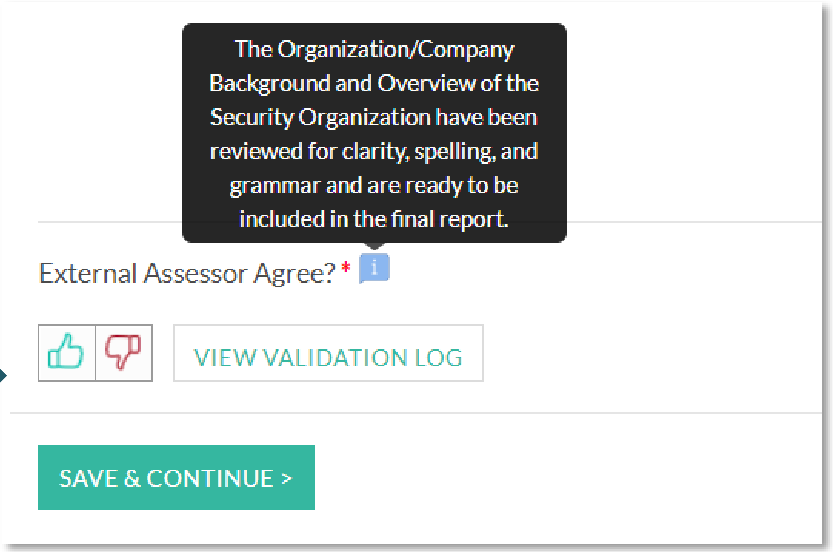
The assessment will remain read-only to the External Assessor until all the Pre-Assessment pages have been approved.

Instructions: How to Review the Pre-Assessment Webforms

Step 1 – After the Assessed Entity has submitted a domain or the entire assessment to the External Assessor, the External Assessor should access the assessment in MyCSF and, within the assessment object, navigate to the Organization Information webform.

After reviewing the Organization / Company Background and Overview of the Security Organization for clarity, spelling, and grammar the External Assessor should click the button to indicate that the content is ready to be included in the final report or the button to indicate that the content should be edited by the Assessed Entity.



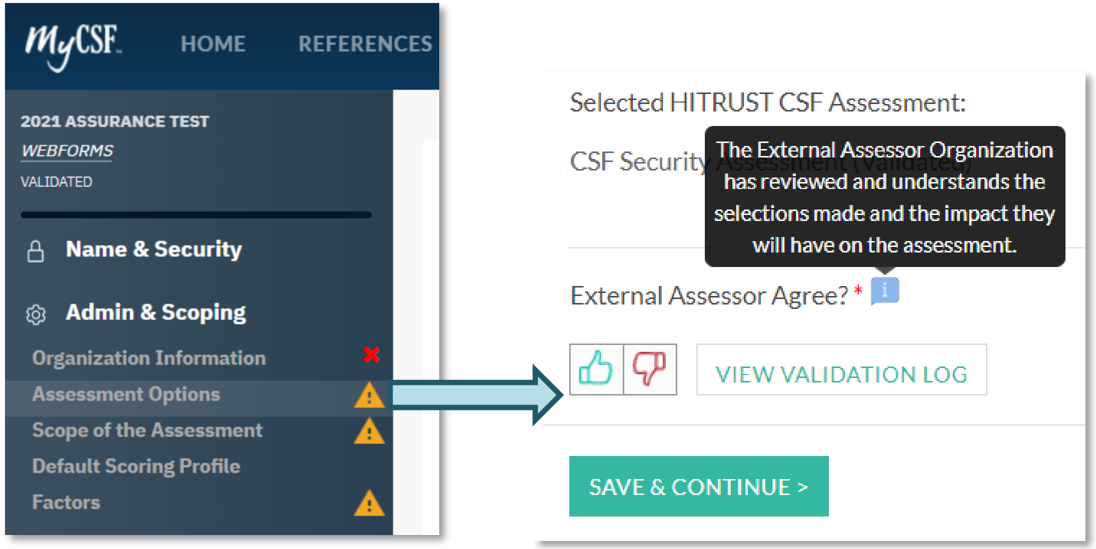


Note: *If the content is not approved, provide a rationale for disagreement to tell the Assessed Entity which updates are needed.*

Instructions: How to Review the Pre-Assessment Webforms

Step 2 - The External Assessor should navigate to the Assessment Options page.

After reviewing the selections made by the Assessed Entity on the Assessment Options page, the External Assessor should click the button to indicate that they have reviewed and understand the selections made and the impact that they will have on the report or the button to indicate that there is a selection should be edited by the Assessed Entity.

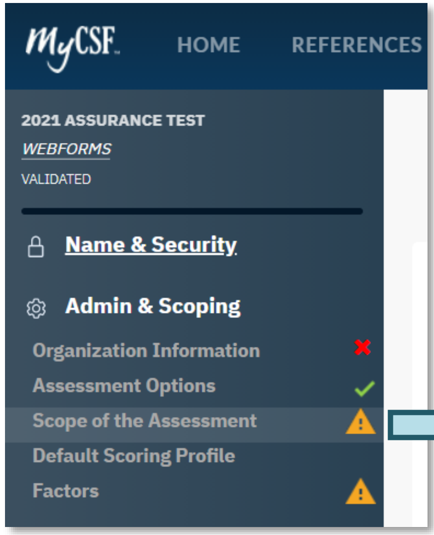


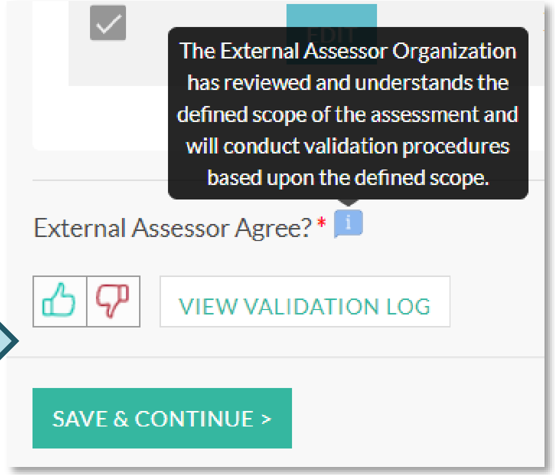
Note: *If the selections are not approved, provide a rationale for disagreement to tell the Assessed Entity which updates are needed.*

Instructions: How to Review the Pre-Assessment Webforms

Step 3 - The External Assessor should navigate to the Scope of the Assessment webform.

After reviewing the platforms/systems, facilities, and services outsourced entries within the Scope of the Assessment webform, the External Assessor should click the 👍 button to indicate that they have reviewed and understand the scope of the assessment and will conduct validation procedures based upon the defined scope or the 👎 button to indicate that there is scoping information that should be edited by the Assessed Entity.



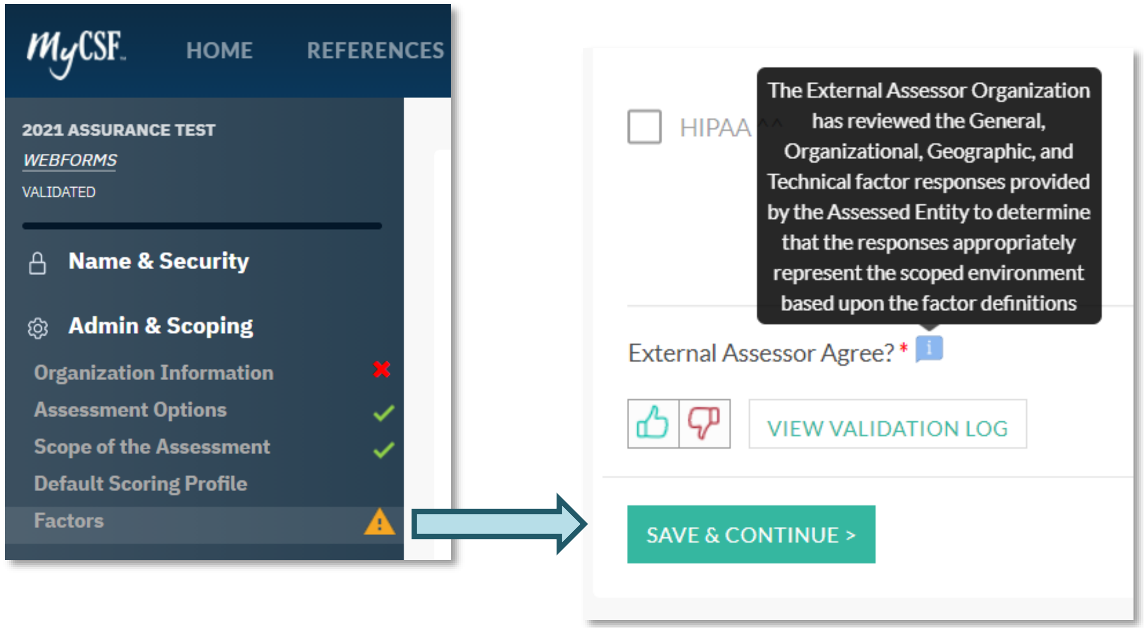


Note: *If the scope of the assessment is not approved, provide a rationale for disagreement to tell the Assessed Entity which updates are needed.*

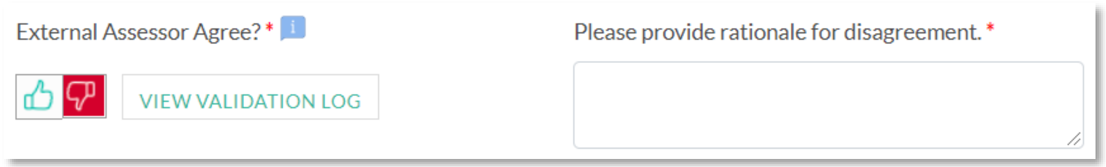
Instructions: How to Review the Pre-Assessment Webforms

Step 4 - The External Assessor should navigate to the Factors page.

After reviewing the factor responses entered by the Assessed Entity on the Factor page, the External Assessor should click the button to indicate that they have reviewed the factor responses and have determined that they appropriately represent the scoped environment based upon the factor definitions or the button to indicate that there is a factor response that should be edited by the Assessed Entity to better represent the scoped environment.



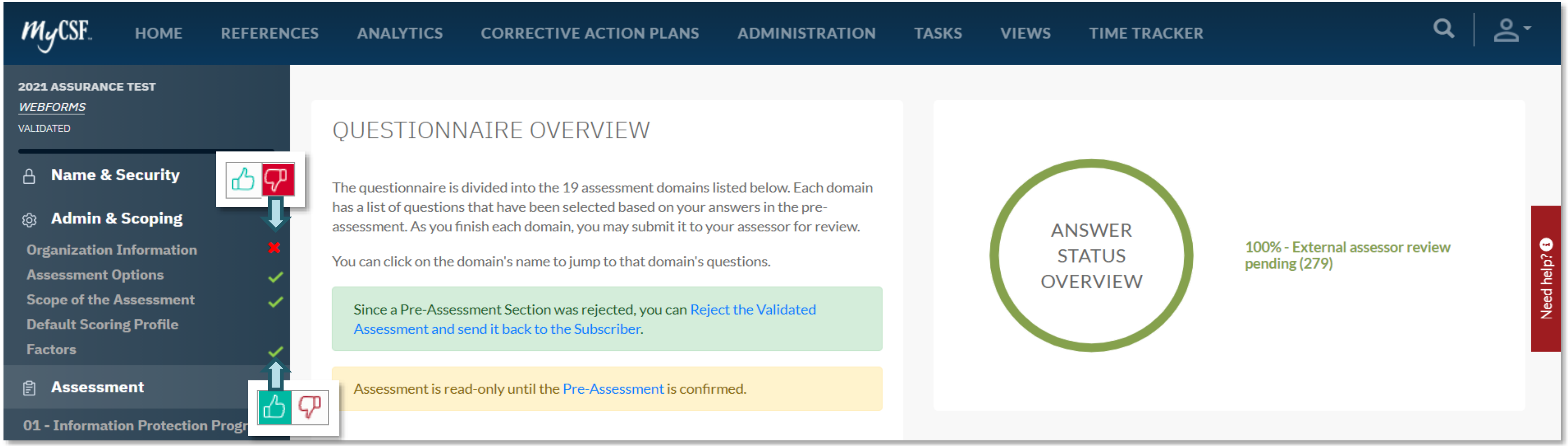
Note: *If the factor responses are not approved, provide a rationale for disagreement to tell the Assessed Entity which updates are needed.*



Instructions: How to Review the Pre-Assessment Webforms

Step 5 – As the External Assessor reviews the Organization Information, Assessment Options, Scope of the Assessment, and Factors, the results of the review will be indicated by if the page was not approved or by if the page was approved.

If any Pre-Assessment section was not approved, the External Assessor will see a link on the Assessment Homepage to *Reject the Validated Assessment and send it back to the Subscriber*. The External Assessor should click this link to send the assessment back to the Assessed Entity for necessary updates. The assessment will return to the *Answering Assessment* phase when rejected.



Instructions: How to Review the Pre-Assessment Webforms

Step 6 – After the Assessed Entity has made necessary updates to the Pre-Assessment sections and submitted the assessment back to the External Assessor, the External Assessor should review each Pre-Assessment section previously rejected. Once all Pre-Assessment sections have been approved by the External Assessor, the assessment will no longer be read-only, and the External Assessor may validate scoring.

Note: *If any sections are not approved by the External Assessor after resubmission by the Assessed Entity, the External Assessor can thumb down the Pre-Assessment and reject the assessment again. This can happen as many times as needed until the External Assessor has approved each pre-assessment section.*