NIST 800-171

User Guide

Date	Change	Authorized
2/18/2018	Initial version (v1.0)	Steven Senz
4/15/2018	Updated manual to reflect new user interface for control and requirement modules – data input schema	Steven Senz
10/20/2020	Included attachments, hints, more key personnel, POA&M export FAQs	Steven Senz
11/11/2020	POA&M Filtering	Steven Senz
2/26/2021	Corrected bad hyperlinks	Steven Senz

Contents

Introduction

ASCERTIS stands for **A**utomated **S**ecurity **CERT**ification of **I**nformation **S**ystems. ASCERTIS is a web-based application that follows the Risk Management Framework mandated by the Federal Government to assess and accredit federal information systems. It is also available for commercial information systems for businesses that provide contractors to the Government.

The Government requires evidence that the ATO letter is based on a critical review or test of the controls and an assessment of the security posture of the system based on those tests.

ASCERTIS provides all the key artifacts to show an auditor that due diligence is followed as required by the Risk Management Framework.

ASCERTIS follows the RMF six-step process.

The Risk Management Framework starts by categorizing the information system as low risk, moderate risk, or high risk, depending on the impact the failure or compromise of the system has on the organization or its mission. The impact of failure is usually based on the type of information processed, transmitted, or stored. The more sensitive the information, the more risk there is should information become compromised.

Once the risk category is determined (step 1), the appropriate security control can be selected to protect the information and the information system (step 2).

By definition, the information of concern is Controlled Unclassified Information (CUI). Information of this type includes, but is not limited to: employee salary and health information, employee background checks, drug testing, company financial records, contract information, and trademark and patent information.

Therefore, this is a moderate-risk system and controls are already defined by NIST SP 800-171 R1 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. ASCERTIS simplifies the first two process steps by identifying all the necessary controls that need to be considered, as well as how these controls are implemented.

The control implementation module (step 3) provides the assessor with an easy-to-select control implementation choice in a good/better/best selection process. If none of the choices reflect how the control is implemented for that system, a custom input field is provided.

In the security assessment module (step 4, part 1), each control undergoes a series of reviews to confirm that the security functions are in place and working as designed. These reviews could be interviews with key security or operations personnel, documentation reviews for policies and procedures, demonstrations of functionality (e.g., password complexity), and reviews of artifacts (e.g., logs, reports, scan results) that are to be produced as a result of monitoring and control.

In the threat assessment module (step 4, part 2) the ISSO/ISSM discusses the impact of various threat impacts to the business mission or the information system. A likelihood rating is obtained based on the rigor of the controls that are in place to prevent the threat from occurring. This rating determines which failed or partially satisfied controls need remediation.

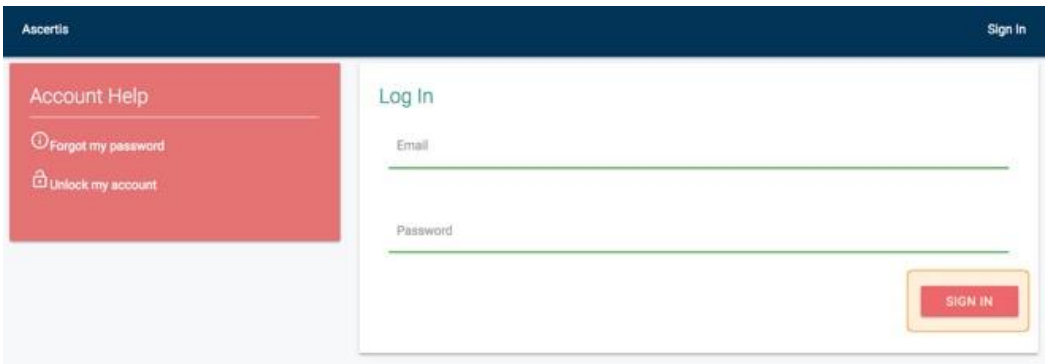
The POA&M report is an agreement between the security team and the operations team on how to remediate controls that put the information system at moderate or high risk. The POA&M, along with a certification letter, are presented to the Authorizing Official who issues the Authority to Operate (step 5).

Over time, the POA&M report is updated to reflect corrective actions to failed controls. Corrected controls are closed out on the POA&M report as part of the monitoring phase (step 6). During this phase, additional inspections may result in new findings. New findings are added to the POA&M list as part of continual monitoring and assessment.

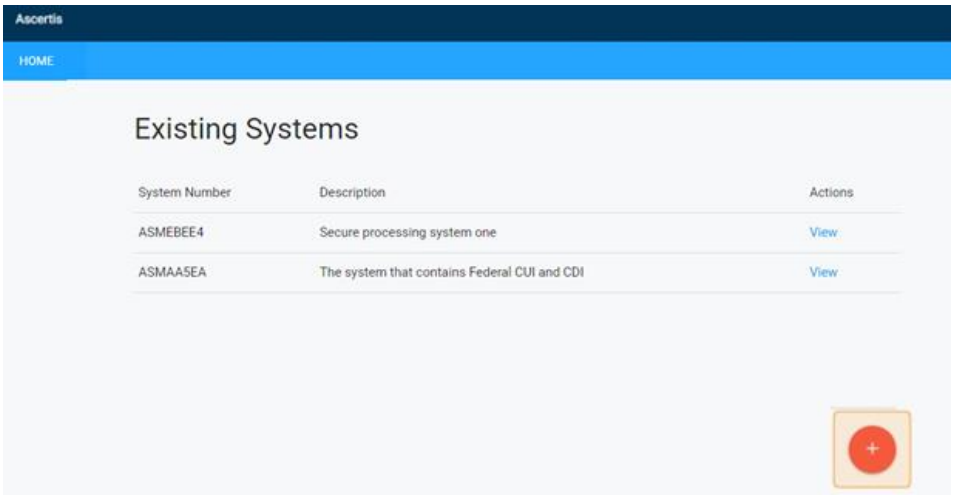
Creating Systems
(for administrators only)

The splash page explains the importance of an independent CMMC assessment for companies that contract with the Department of Defense.

Click "Sign In" to enter the login page.



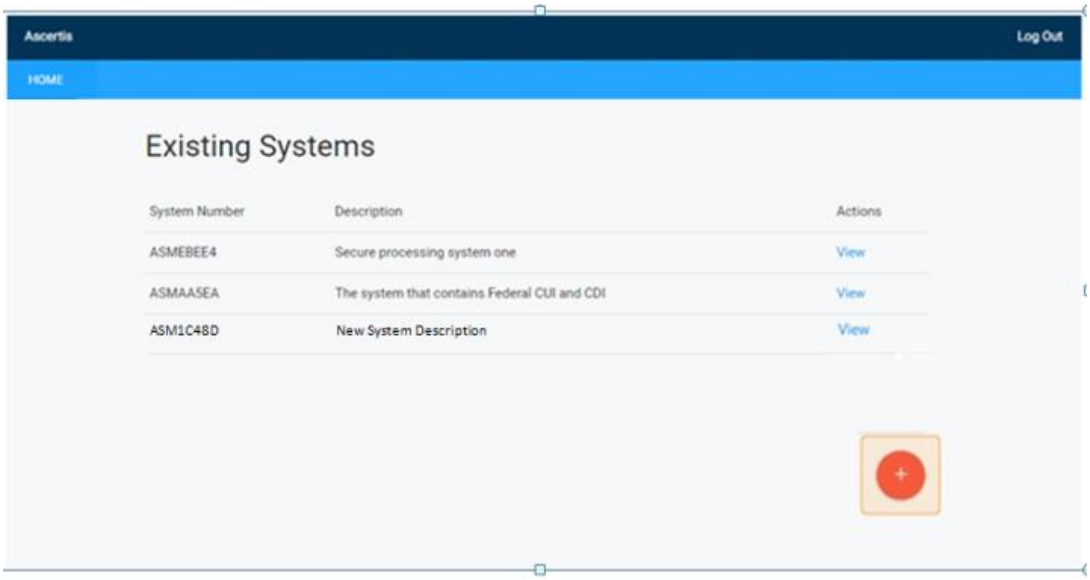
Enter the username and password to sign in. A pop-up appears to indicate a successful sign in.



The Existing Systems page opens, showing the available systems, named with an alphanumeric identifier and description.

Click “+” to add a new system/organization.

Type in the system/organization name and description, then click “Submit.”

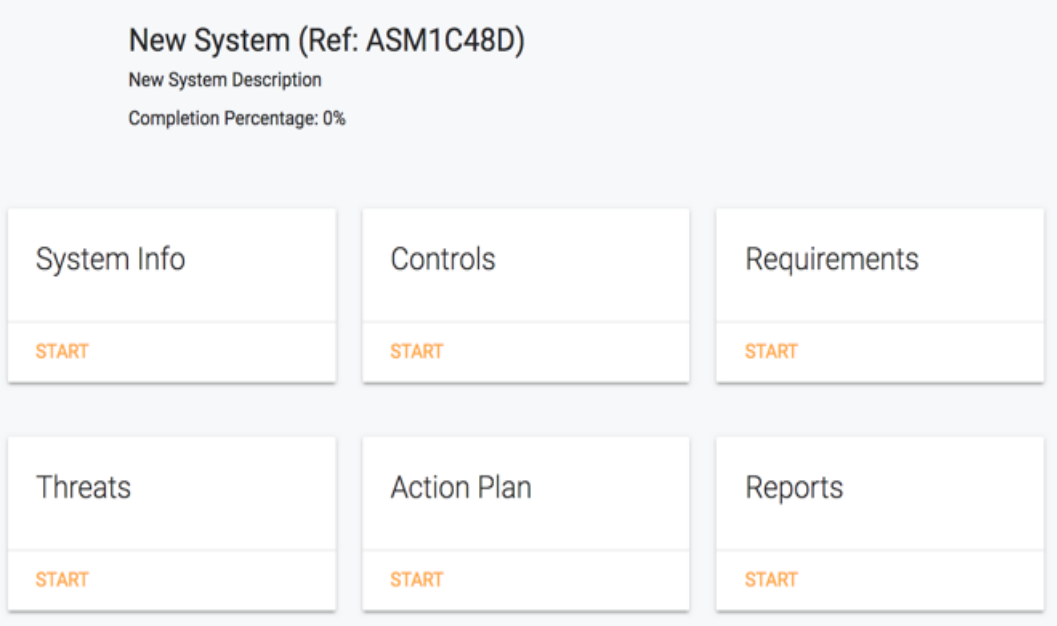


The Existing Systems page refreshes. Click “View” to access the eight modules for the selected system.

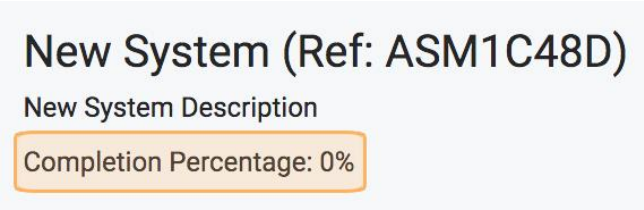
ASCERTIS Modules

ASCERTIS contains six modules: System Info, Controls, Requirements, Threats, Action Plan, and Reports.

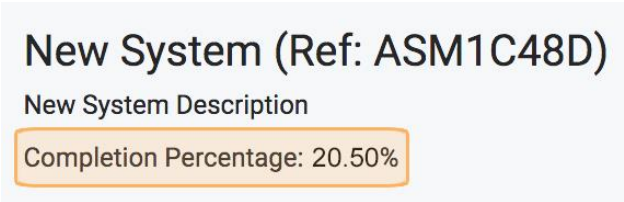
These modules appear on the system home screen. The system name appears at the top, followed by its alphanumeric reference code.



The module completion percentage begins at 0%.



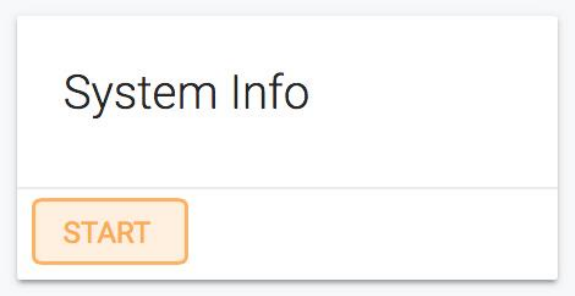
As the modules are completed, the percentage increases.



Complete the modules in sequence from left to right, starting with System Info and ending with Reports. Save the assessment process at any point and continue later by clicking “Start” on the module of interest.

Users should note that the Threat module is locked until the Controls and Requirements modules are completed. This is to prevent the generation of “misleading information” due to control and requirement information not being entered.

The Action Plans module is locked until the Controls, Requirements, and Threat modules are completed. This is to prevent the generation of POA&M items for requirement for which the calculated risk is determined to be low.



Navigate back to the home screen by clicking on the system reference code, located in the center of the navigation bar at the top of the screen.

To log out, click “Log Out” on the right side of the navigation bar.

Preparing for the Assessment – Graphics and Lists

There are several items that need to be prepared before the assessment engine is ready to be used. These are:

1. A company logo
2. Network diagram showing all the interfaces to repositories (local and remote)
3. Hardware list
4. Software list

The company logo needs to be a at least 120 KB in size. The network graphic should be at least 450 KB. The network diagram should not exceed one page. The hardware list must contain the following headers. The hardware template can be downloaded from the following link and should look like the template below.

https://ascertis.solutions/ascertis-equipment-list-template

A	B	C	D	E	F	G	H	I	J	K	L
IP_Address	Host Name	Description	OS_Family	OS_Name	OS_Version	Patch Level	Manufacturer	Model	MAC_Address	Equipment_Class	Serial_No

Below is an example of how the equipment list should be completed. Note that, due to the size, the file records are shown in two parts.

A	B	C	D	E	F
IP_Address	Host Name	Description	OS_Family	OS_Name	OS_Version
192.101.6.107	APPVOLTEST-01	Server	ubuntu	ubuntu_linux	12.04
192.101.0.59	DWESA006FA81045	Router	Cisco	cisco:ios:15	S
192.1.1.187	FLB-B148069	Workstation	Windows	windows_10	sp1:x64-enterprise

G	H	I	J	K	L
Patch Level	Manufacturer	Model	MAC_Address	Equipment_Class	Serial_No
4	HP	2020	00:50:56:ac:44:49	Server	ABEX-1376-1f25
15.8	CISCO	5750	00:27:90:ad:589:890	Router	ABEX-1376-1f42
1909	Dell	Optiplex 750	ec:cd:6d:85:10:b8	Workstation	ABEX-1376-1f127

Only the first three columns (IP address, Host Name, and Description) must be completed. The other columns are optional but provide a more complete picture of the infrastructure environment.

The software template can be downloaded from the following link and should look like the template below.

https://ascertis.solutions/ascertis-software-list-template/

A	B	C	D
Name	Vendor	Version	Patch_Level

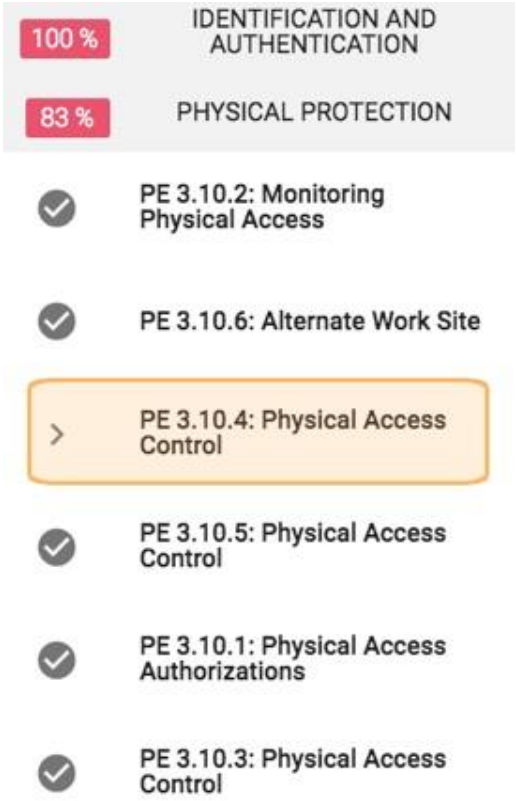
Below is an example of how the software list should be completed. Only the first three columns are mandatory.

A	B	C	F
Name	Vendor	VERSION	Patch_level
DesignPro	Capterra	5	5.5.708
Adobe Acrobat XI Pro	Adobe	11	11.0.19
Adobe Flash Player	Adobe	26	26.0.0.131
Adobe Photoshop CC 2015	Adobe	2015	16.1.2
Adobe Reader XI (11.0.20)	Adobe	XI	11.0.20

Progress Sidebar

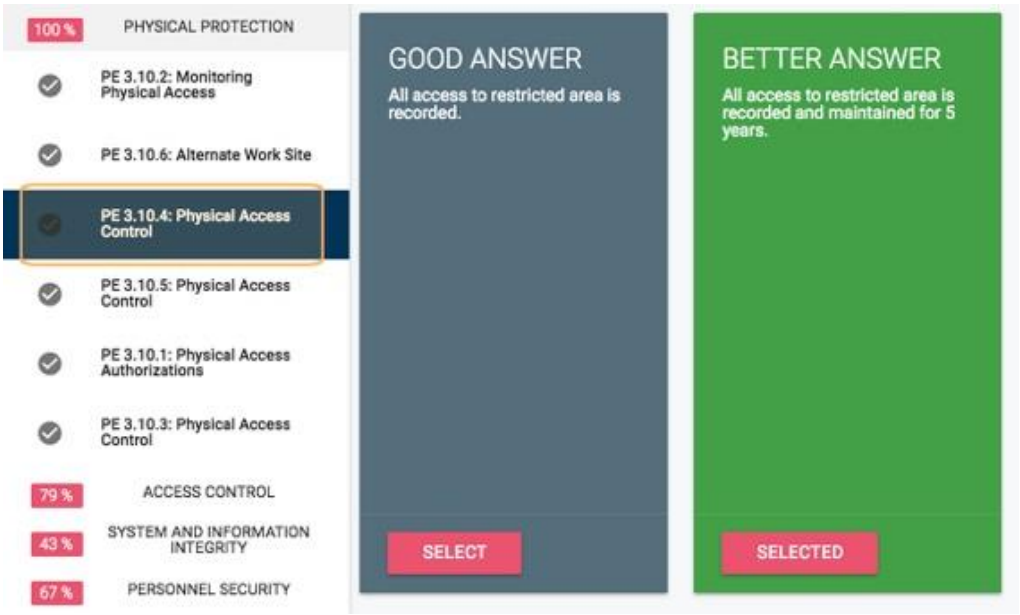
As controls are selected, the percentage meter on the left reflects the overall progress. When the meter reaches 100%, all the controls have been mapped to an implementation method.

Notice the controls within each security domain have their own percentage of completion. This percentage reflects the number of controls that have been addressed out of the total number of controls in that domain. For example if there were 10 controls in the domain and 7 have been addressed the completion percentage would be 70.

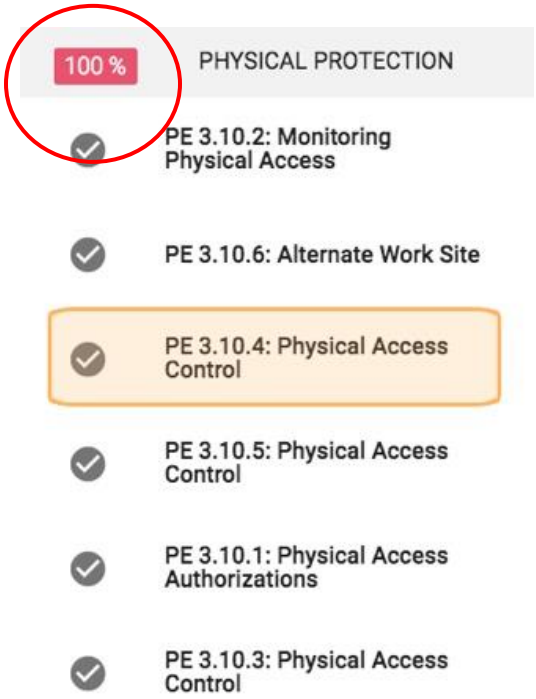


Click on the heading name to expand the controls. Completed controls show a checkmark. All sub-heading controls must be completed for the heading control to show 100%.

In this example, PE 3.10.4 does not have a checkmark, so that control needs to be entered.



Click on the name of the control to generate the good/better/best options. Select the best option, or type a customer answer.

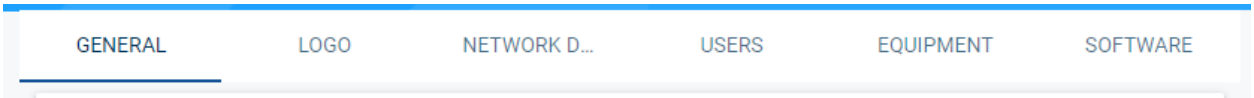


The progress sidebar updates to reflect the current percentage completed.

Manually move to the previous or next control by clicking its number on the progress sidebar. All control answers must eventually reach a completion percentage of 100% before moving onto the next module.

Module 1 – System Information

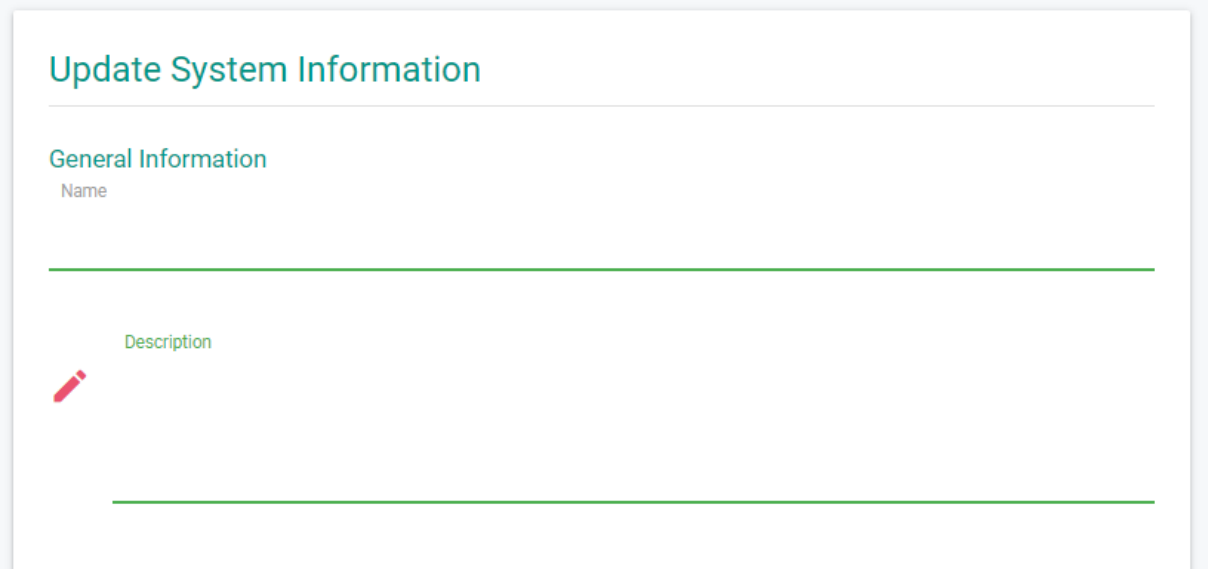
The System Information module creates the front matter of the System Security Plan. It collects all the basic information of the system and the organization, such as the key stakeholders, the environment, mission, and boundaries. The information to be collected appears in the top menu bar for this module. This includes general information about the system, a company logo, a network diagram, who the key users of the system for the assessment are, and the equipment that will be covered by the assessment. The information is completed by selecting the categories in the menu bar at the top.



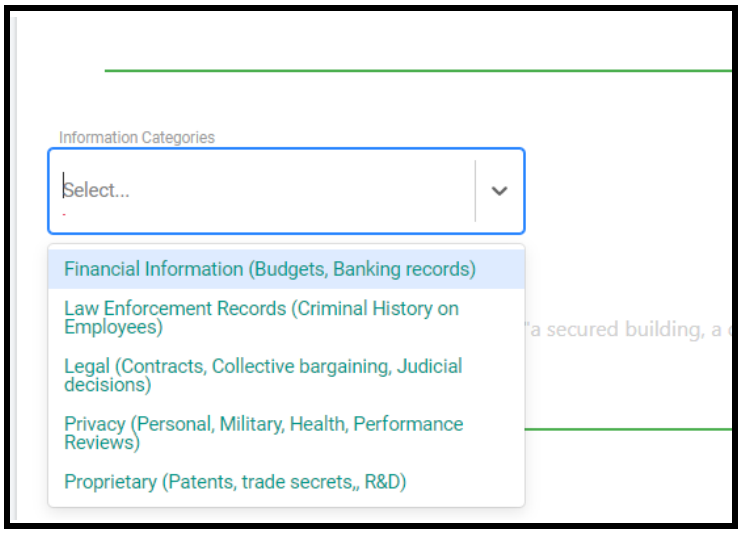
The Name of the system will be auto inserted from the name given during system identification by the administrator.

GENERAL

In the Description field, there should be a brief description of physical and logical components of the systems.

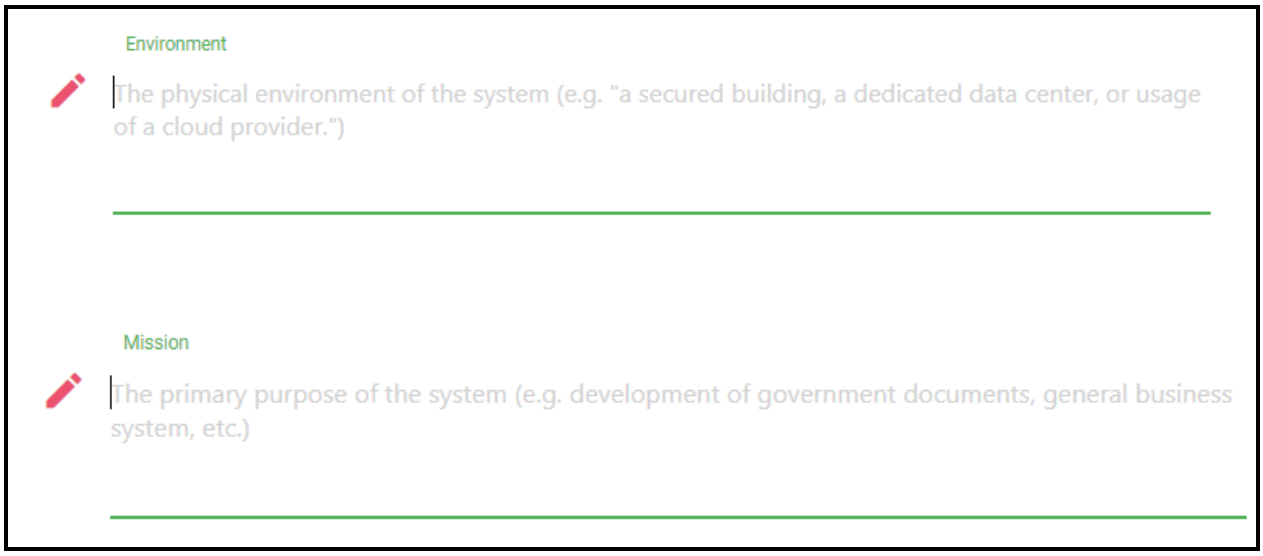


Because the assessment is concerned with the protection of Controlled Unclassified Information (CUI) and Technical Design Information (TDI), these categories of information have been loaded into the application.

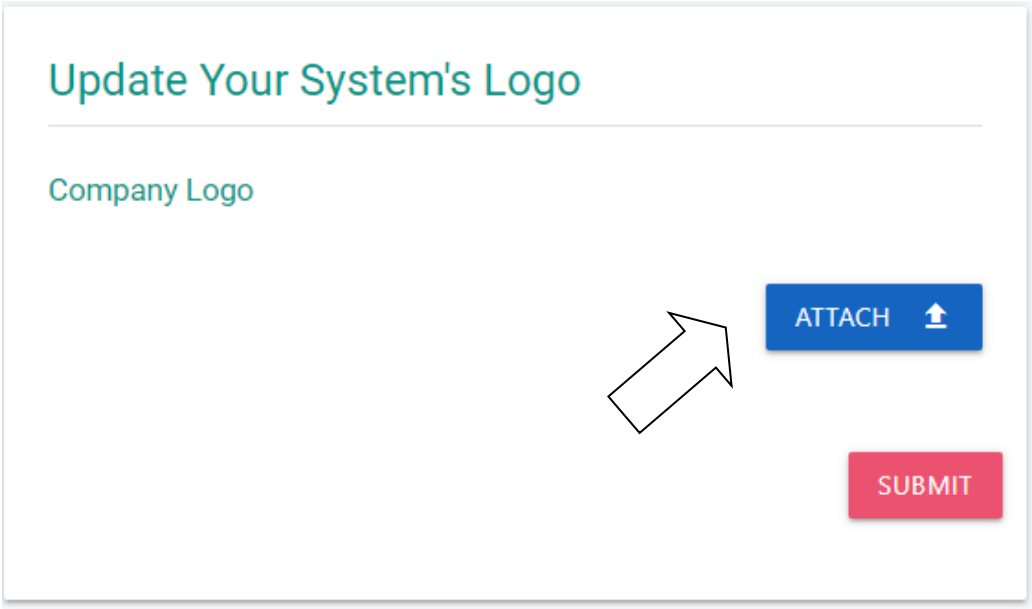


Click on “Information Categories” to select the information types. Use the drop-down menu to select the information category, entering more than one category, if needed.

Next, enter the Environment of the IT system and the Mission (primary purpose) of the system. The pencil icon will turn red to indicate that text is being entered. Indicate if there is another system connected to the system under review (ISA) and the security level of the connected system.

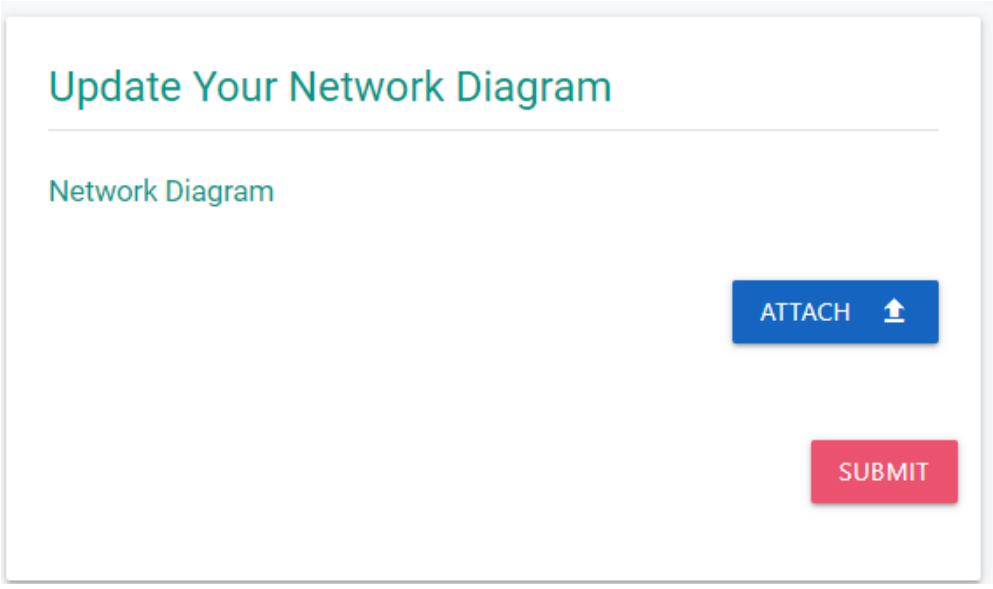


LOGO



Select a company logo by clicking on "Attach" to upload the company logo just selected. Then click "Submit." The company logo graphic appears on the cover of the reports. The logo should be a high-resolution image, typically 3 inches by 3 inches. Graphics for the diagram and logo must be in PNG or JPEG format.

NETWORK DIAGRAM



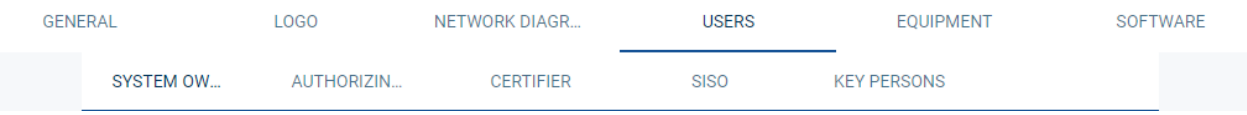
Follow a similar process for the company logo. Select a network diagram file from your repository. Click "Attach" to upload the diagram, then "Submit." Diagrams should show the border firewalls, the servers, routers, and endpoints. The network diagram format must be GIF or JPEG. If there is a cloud server in the architecture, include a VPN link to the service provider.

USERS

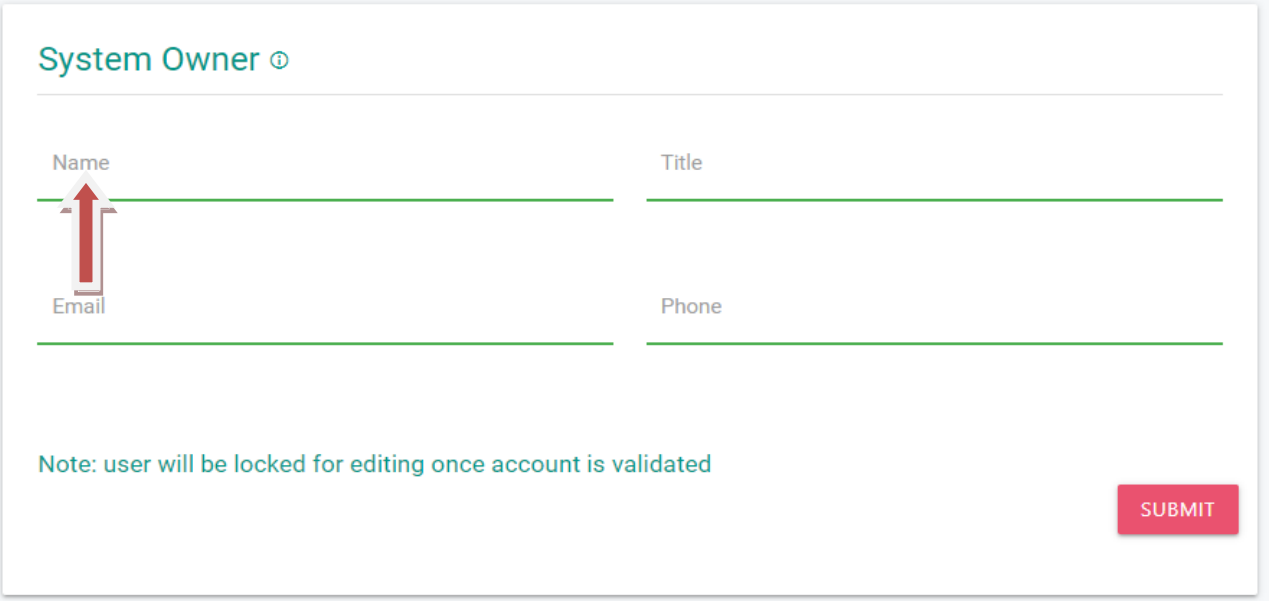
In this section, there are a series of input tiles for the various personnel responsible for the security of the information and assessing the organization and the Information System. These personnel roles include:

System Owner
Certifier
Authorizing Officer
Senior Information Security Officer
Key Person

The user inputs information into the tiles by navigating the user menu at the top. The first tile listed is the System Owner.



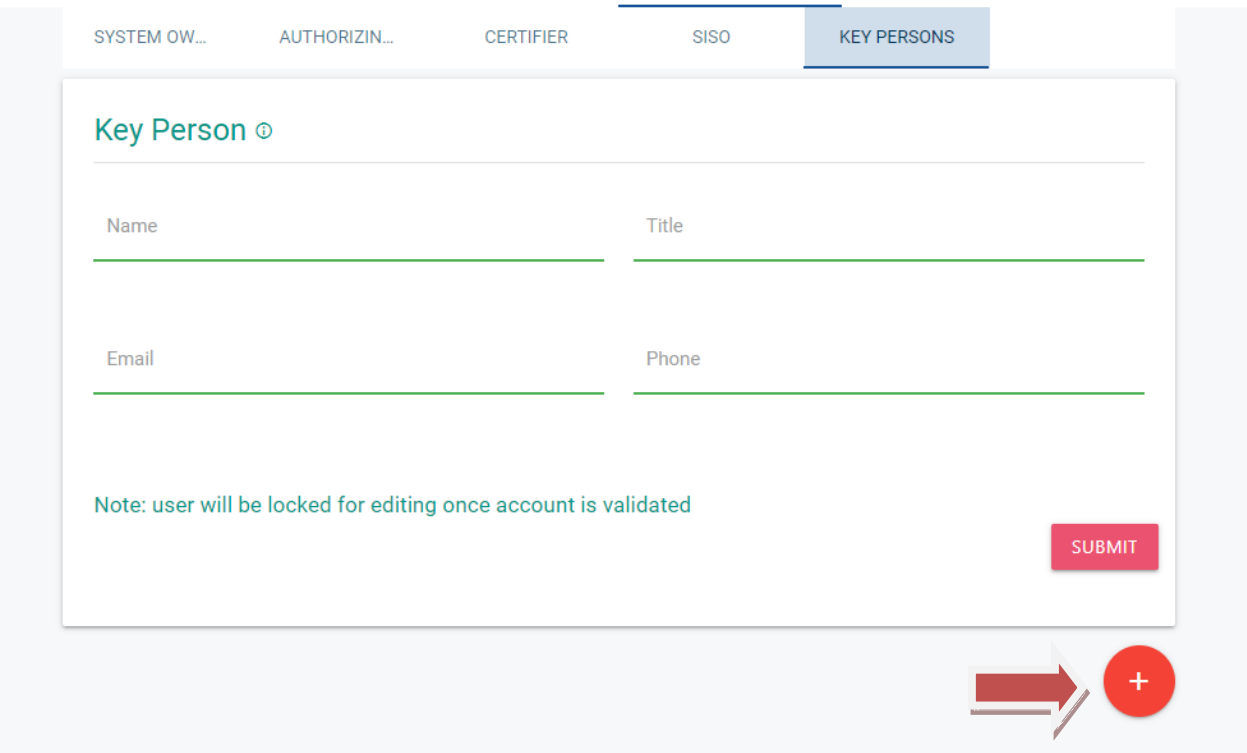
The input tiles all require the same information. Below is the input tile for System Owner.



The definition of each user is defined in the information circle next to the role title. Hovering the mouse over the information circle displays the definition. Information is entered by placing the cursor on the line under each input field.

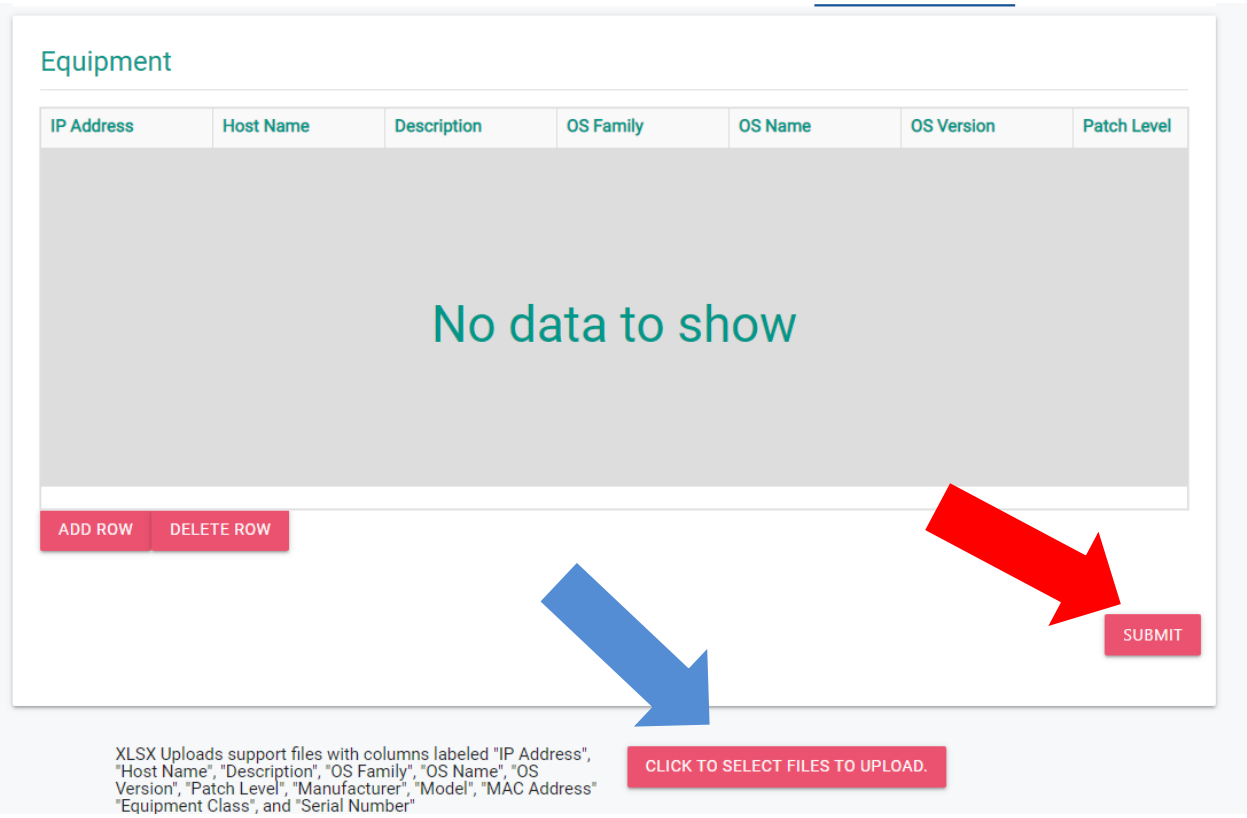
The Key Person field:
The Key Person is usually someone in the organization that does not have cyber responsibilities but performs control functions that are necessary for information assurance. The head of Human Resources is usually the entity performing background checks on new or current employees. The Facility Director is usually responsible for the close circuit TV, or the physical security locks, and other mechanisms that physically secure the environment. As such, there is an option to add more than one Key Person.

After the information is entered for the first individual, click the "+ button" in the lower right-hand corner. A second tile will appear underneath the one just completed. If additional key people are needed, continue to select the "+ button."



EQUIPMENT

The information about the equipment included in the assessment can be either entered by hand using the “Add Row” button or by uploading a CSV file with the requisite information. If your information is contained in a CSV file, click on the red button at the bottom (blue arrow), select the appropriate file, which will appear in the table, then click “Submit” (red arrow).



While not all information is required, it will be useful for monitoring the environment during the monitoring stage of the Risk Management Framework.

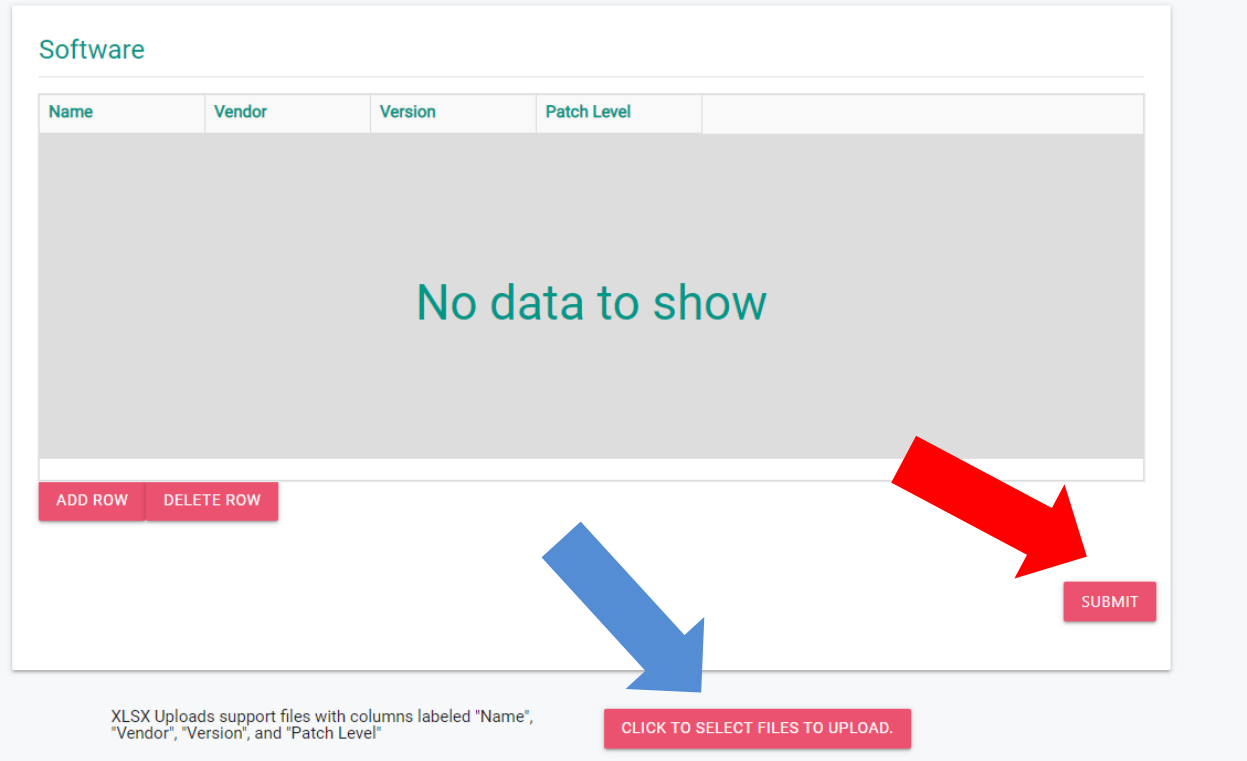
If adding information by row, double click on each cell to bring up the input form. Enter text fields within tables for the operating systems, hardware and component inventory, and major applications used. Tabbing over places the cursor in the next column on the table. To create a new row, click “Add.”

Click “Submit” to save and return to the home screen.

To modify the prior inputs, click “Start” on the System Info module. Enter the updated information into the input fields and click “Submit” to save over the prior selections.

SOFTWARE

The information about the software included in the assessment can be either entered by hand using the "Add Row" button or by uploading a CSV file with the requisite information. If your information is contained in a CSV file, click on the red button at the bottom (blue arrow), select the appropriate file, which will appear in the table, then click "Submit" (red arrow).

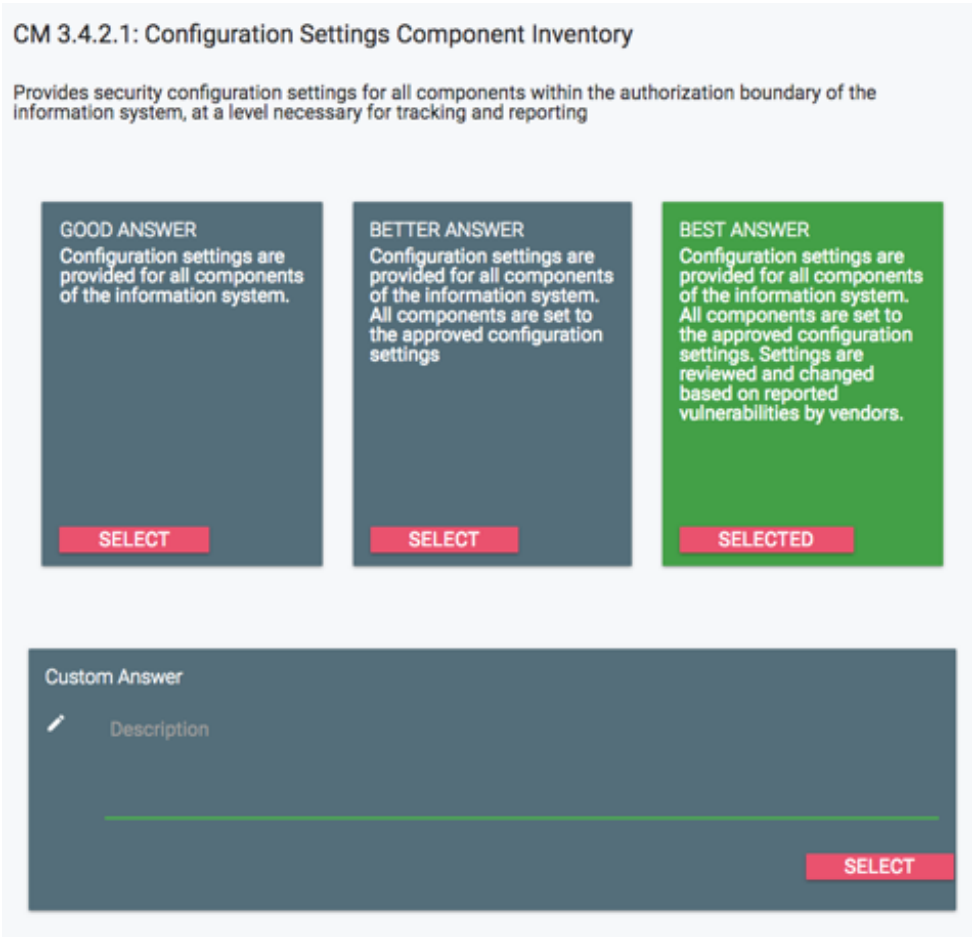


If adding information by row, double click on each cell to bring up the input form. Enter text fields within tables for the operating systems, hardware and component inventory, and major applications used. Tabbing over places the cursor in the next column on the table. To create a new row, click "Add."

Click "Submit" to save and return to the home screen.

To modify the prior inputs, click "Start" on the System Info module. Enter the updated information into the input fields and click "Submit" to save over the prior selections.

Module 2 – Control Implementation



Since by definition this is a moderate-risk system, the controls are already defined. The Control Implementation module provides an easy-to-select control implementation choice in a good/better/best selection process.

After reading the descriptions of the good/better/best answers, click "Select" below the appropriate answer. If none of the choices reflect how the control is implemented for that system, enter a custom answer.

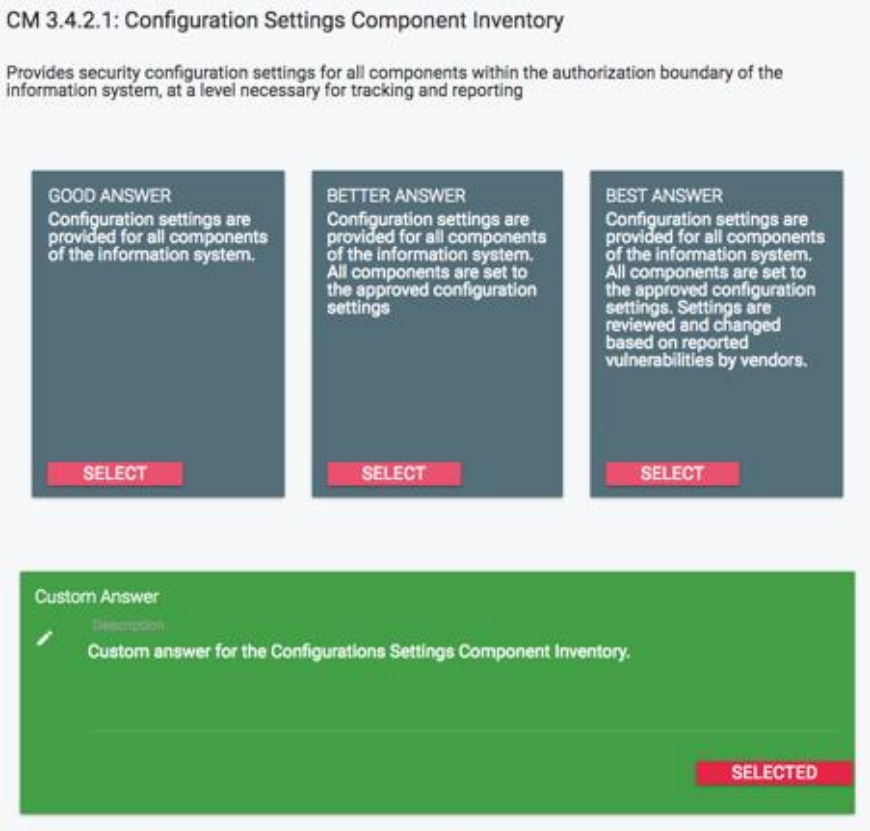
Once an answer is selected, "Select" changes to "Selected," and the blue background changes to green. Change an answer by clicking on "Select." The colors will reflect the new selection.

Note: Custom answers do **not** disappear, even if that answer is no longer selected. This allows for re-selection of that answer in the future without the need to re-type the entire field.

There are 133 basic and derived controls in the NIST 800-171 R1 standard. Some controls may not apply. In this case, enter the words "Not Applicable" in the custom input field.

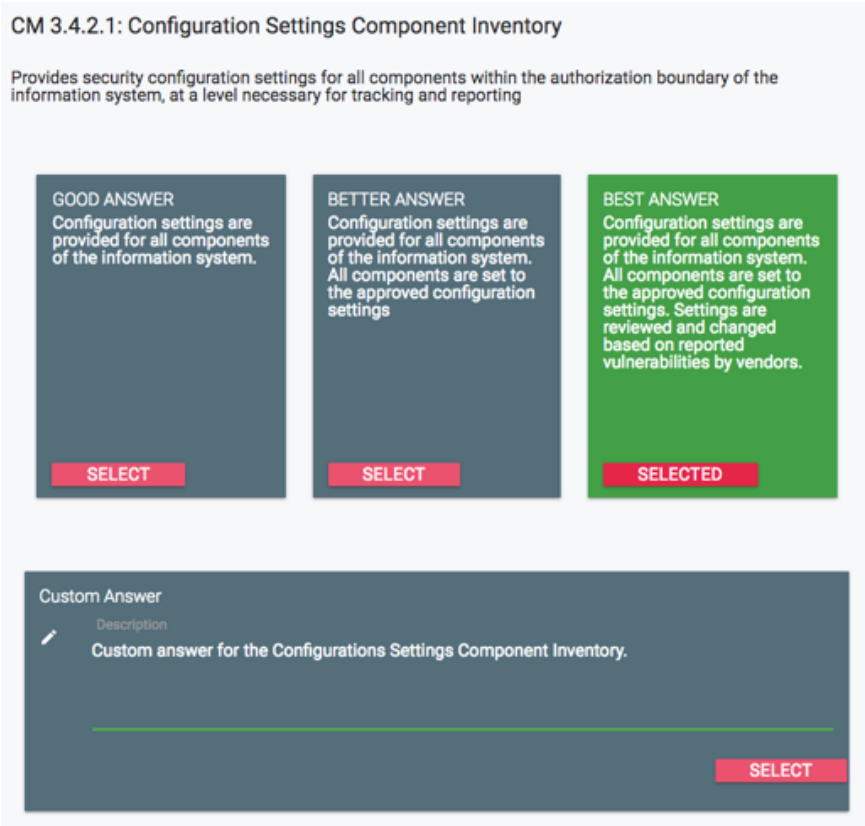
The next control loads automatically after clicking "Select."

Manually navigate to the previous or next control by clicking the forward and backward arrows.

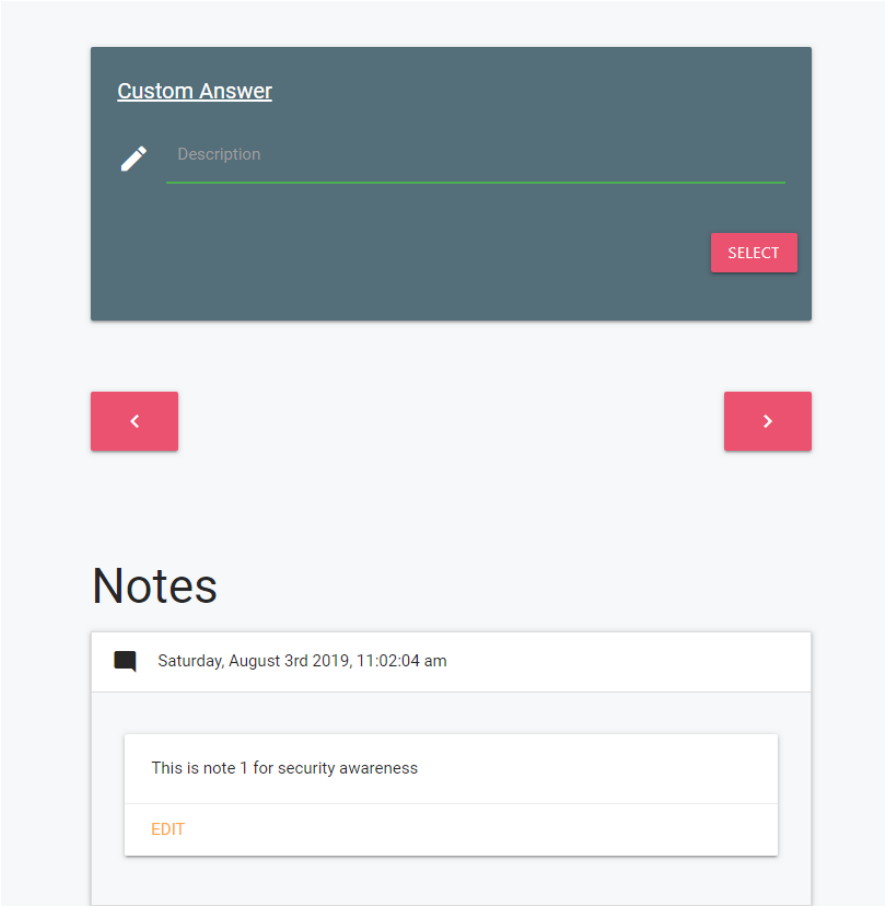


The selected answer is highlighted in green.

Selecting the custom answer will highlight the custom answer in green.



Selecting a new or prior answer will highlight the selected answer in green. The custom answer is still available for the future, even though it is not the currently selected answer.

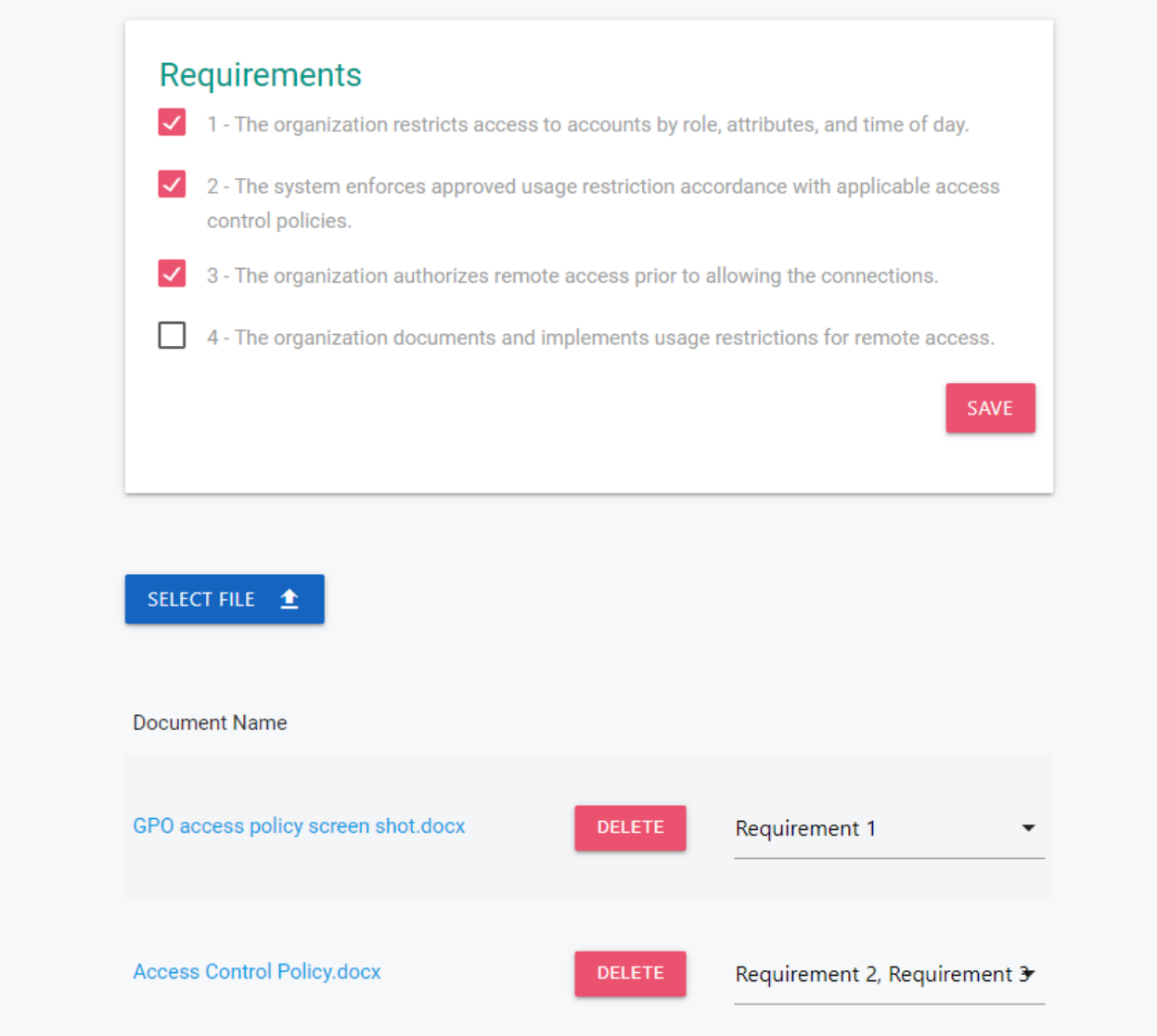


Each control also contains a notes section at the bottom of the control page. The notes section is for additional explanations of how the control works or mitigation plans that are already in progress. Notes for controls will appear in POA&M reports for any control that does not meet all the requirements.

Notes are additive. So assessors/ evaluator can add additional notes for each control. The system keeps track of the time and date of multiple notes.

Module 3 – Requirements

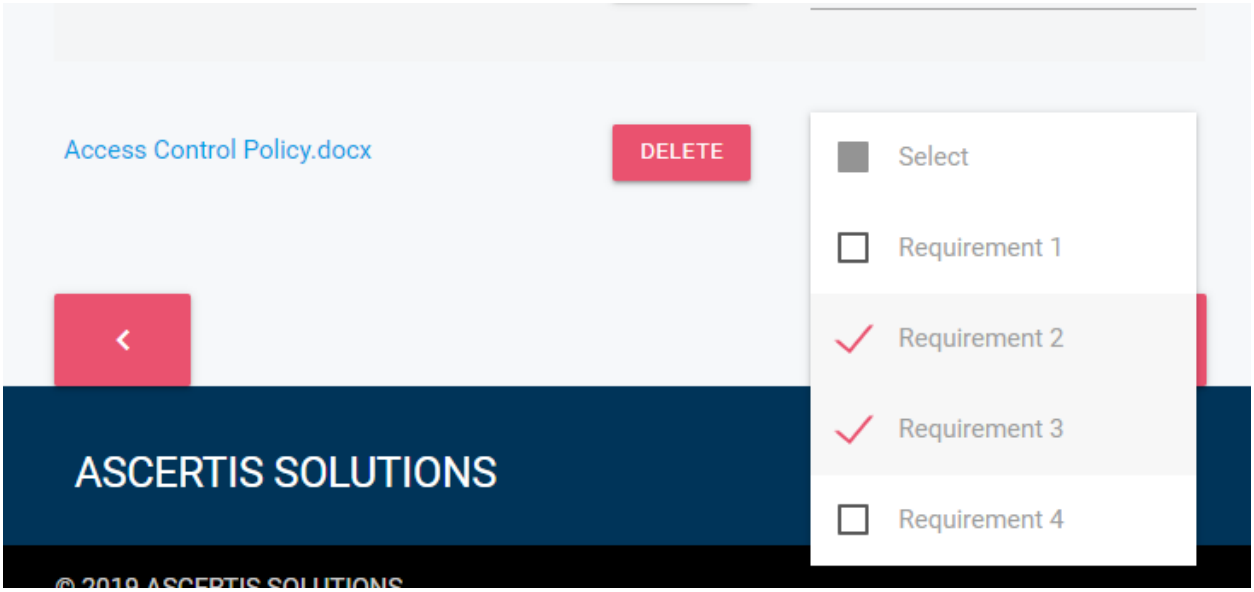
In the Requirements module, the organization's ISSM or designated security individual determines which requirements are satisfied by the implementation of the security control defined in the previous module. Each Control implementation has one or more security requirements it is designed to satisfy. The individual checks the requirements that are satisfied. Requirements that are not met are not checked, and these will result in POA&M items.



Controls have multiple requirements. Each requirement usually requires a separate test/interview/artifact to confirm the requirement met. For each requirement that is checked, the ISSM or security individual needs to ensure that an appropriate artifact can be produced to support the

decision. Artifacts that support the satisfaction of the requirement can be attached to the requirement tile. Simply click on the select button to add an artifact. Once the artifact is attached, use the pull down arrow to indicate which requirements are satisfied. More than one requirement can be satisfied by an artifact.

In the example below, the Access Control Policy satisfied requirements 2 and 3, so both requirements are checked.



During the independent assessment, the certifier(s) will need to review some or all the artifacts to determine the accuracy of the requirements ratings.

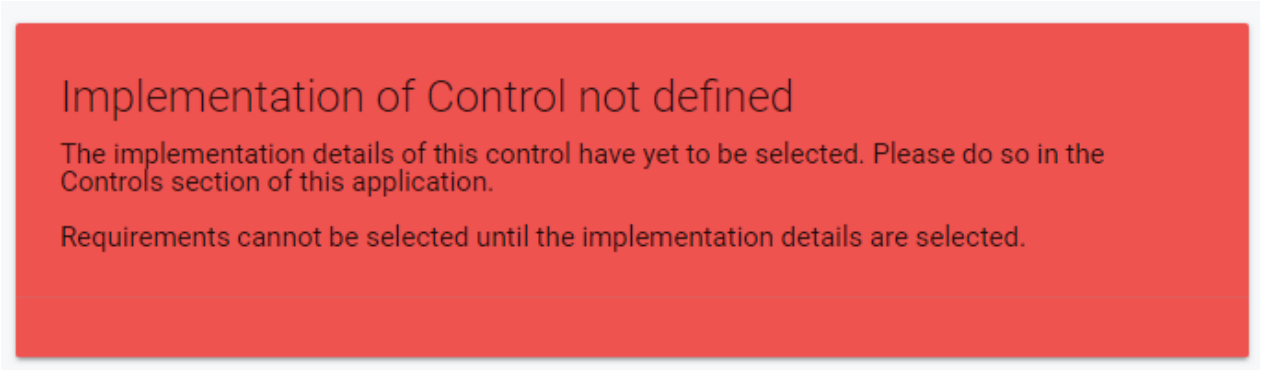
- Requirements that state the organization has a policy require a documentation review.
- Requirements that state a process is followed require a documentation review and an interview with a person who implements that process.
- Requirements that state an artifact is produced (e.g., logs, reports, scan results) require the artifact be produced or shown.
- Technical requirements require either a demonstration (e.g., session timeout in 15 minutes), or evidence that the technical requirement is coded into group policy, firewall policy, or other program code that is implemented to monitor or control the environment.

Several metrics for each control are collected: total requirements satisfied, total requirements not satisfied, and risk rating of the control.

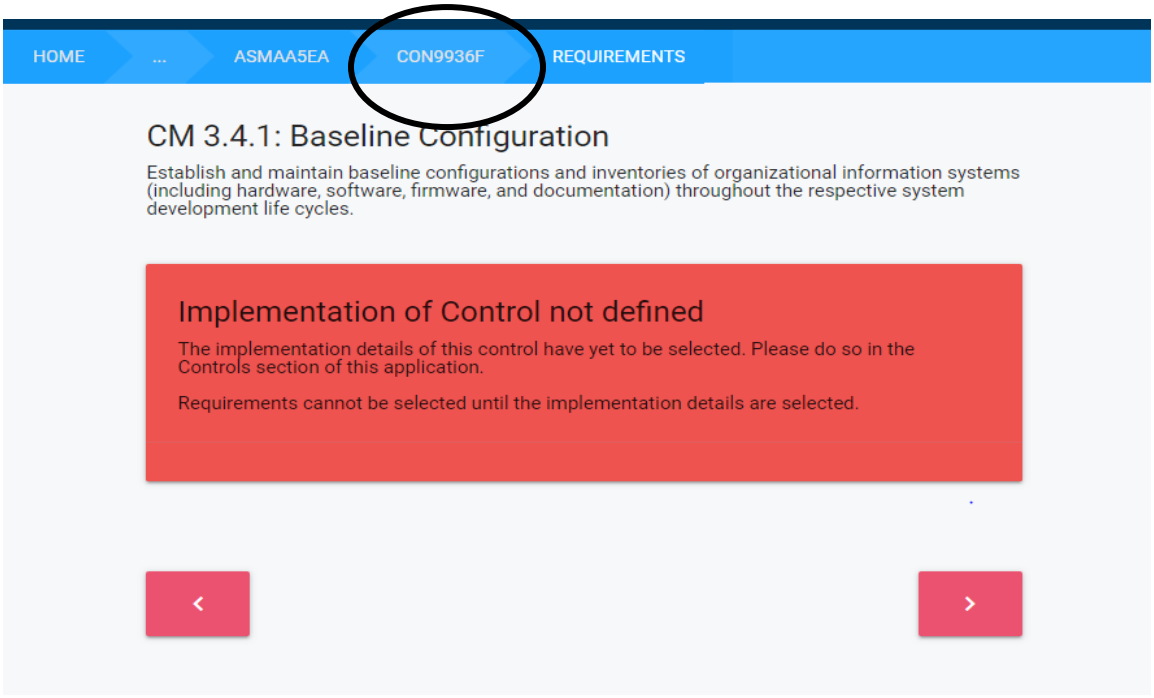
The control is satisfied when **all** requirements are met. Many controls meet some, but not all, of the requirements. The percentage of requirements met determines if corrective actions for that control must be performed. The Threat Assessment section provides more details.

Use NIST SP 800-171A R1 as the guide to determine relevant tests/interviews/artifacts to conduct for each test.

Note: Controls cannot be assessed if they have not been defined as implemented in the previous module. In these instances, a red warning box appears. Return to that control in the Controls module and complete the implementation type. Then the checkboxes for that control in the assessment module will activate.



Click the control link on the menu bar to return to the control.



Module 4 – Threat Assessment

In the Threat Assessment module, the ISSO/ISSM discusses the impact of various threat scenarios to the business mission or the information system. A likelihood rating is obtained based on the rigor of the controls in place to prevent the threat from occurring. This rating determines which failed or partially satisfied controls need remediation.

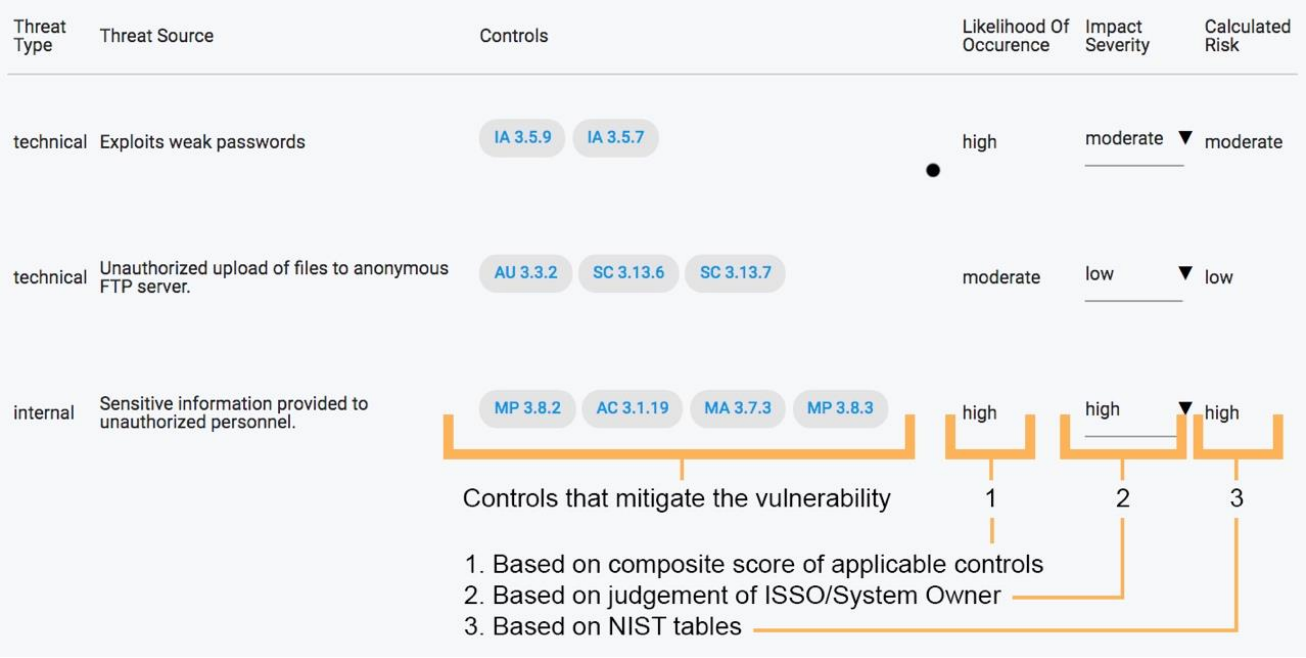
Mapping controls to each threat vector determines which controls to remediate that provide the greatest value.

Calculated risk of moderate and high are forwarded to the POA&M table for remediation.

The threat module discusses multiple threat vectors and scenarios that could compromise the information system or the company and its mission.

The likelihood of occurrence is based on the level of rigor of enforcement by the controls that are implemented to protect the environment from that threat scenario.

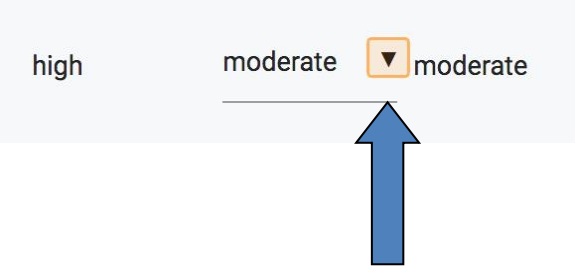
The rigor of enforcement is based on the number of functional requirements satisfied by the group of control (as the numerator) over the total number of functional requirements (as the denominator) that could be satisfied by the group of control.



Likelihood of Occurrence

If 80% of the controls are enforced for a specific threat source, the likelihood of occurrence is low for that attack vector. If 60-79% of the controls are enforced, there is moderate likelihood. If less than 60% of the controls are enforced, there is high likelihood of occurrence. These values automatically appear in the threat table.

Impact severity is a rating decided by the stakeholders of the information system/company.



Select the appropriate impact severity from the drop-down menu.

Choices are low, moderate, or high.

Impact severity is **high** if the event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. Impact severity is **moderate** if the event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. Impact severity is **low** if the event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

The calculated risk is based on the NIST risk table from NIST 800-30 as in the table below.

Calculated risk of moderate or high requires that the controls that help mitigate this risk be improved to cause the overall evaluated risk to become "low." Controls that are not considered low risk are added to the POA&M list.

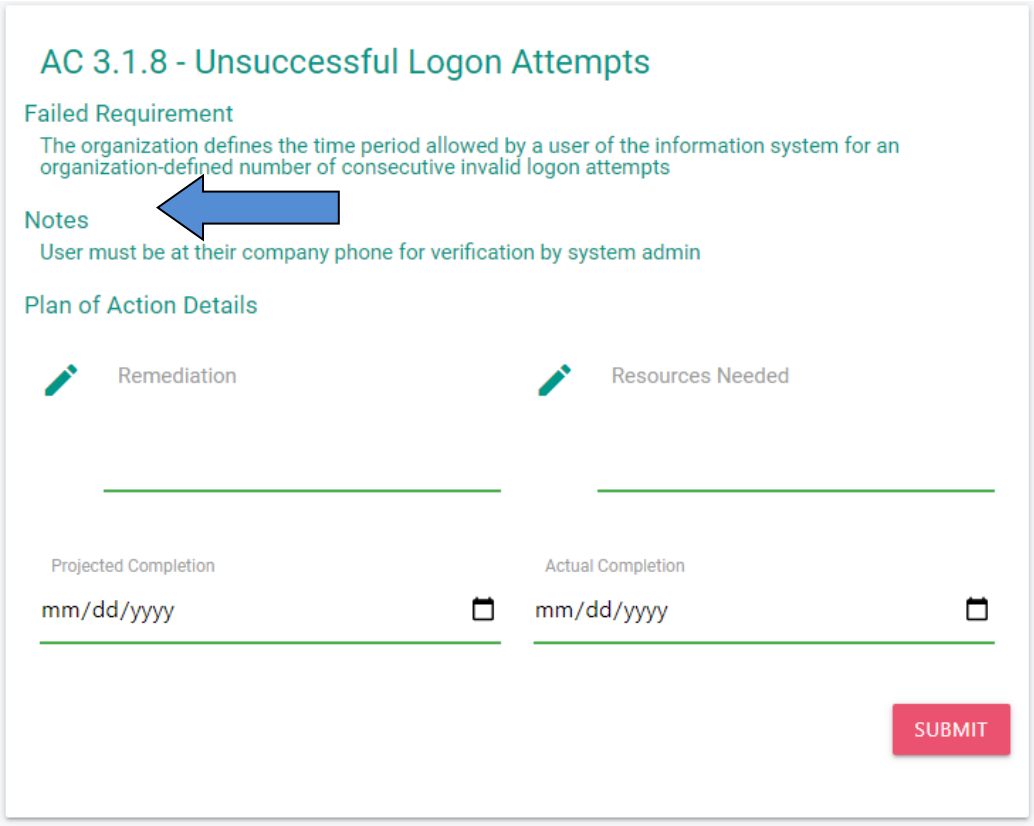
Threat Likelihood	Severity Impact		
	Low	**Moderate**	**High**
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Module 5 – Plan of Actions and Milestones (POA&M)

The POA&M table displays controls needing remediation. It auto-generates this data from the threat likelihood assessment. Thus, the threat assessment module must be completed prior to entering the POA&M module.

POA&M items include remediation strategies, timelines, and points of contact. The ISSO/ISSM is responsible in assuring that these corrective actions take place. The POA&M table auto-generates with respect to the controls included in the table. POA&M items are color coded as follows:

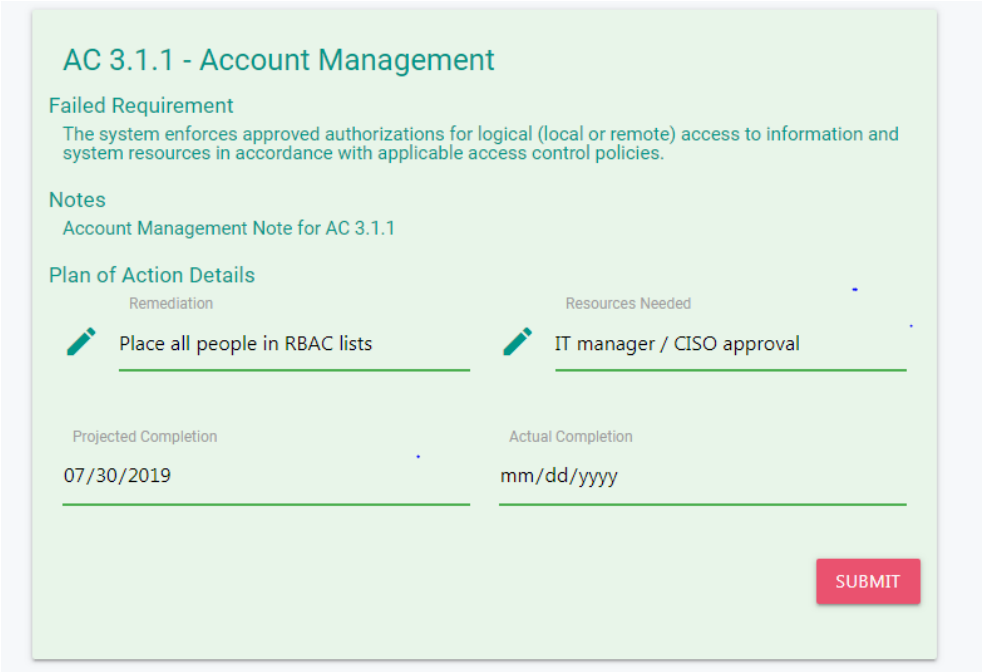
- White – The corrective actions and responsible personnel have not been identified.
- Light Green – Corrective actions, responsible personnel and due date have been identified.
- Dark Green – POA&M actions has been successfully closed out.
- Red – POA&M item due date has passed, and the POA&M action has not been completed.



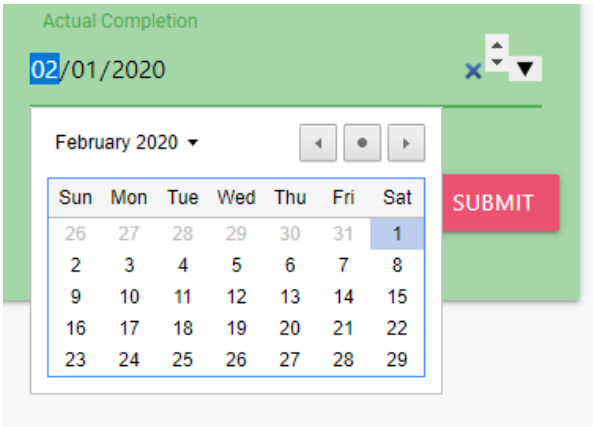
All POA&M item start as white background items.

The ISSM and organizational leadership agree on a corrective action, what resources are needed (personnel, budget, etc.), and the due date for completion.

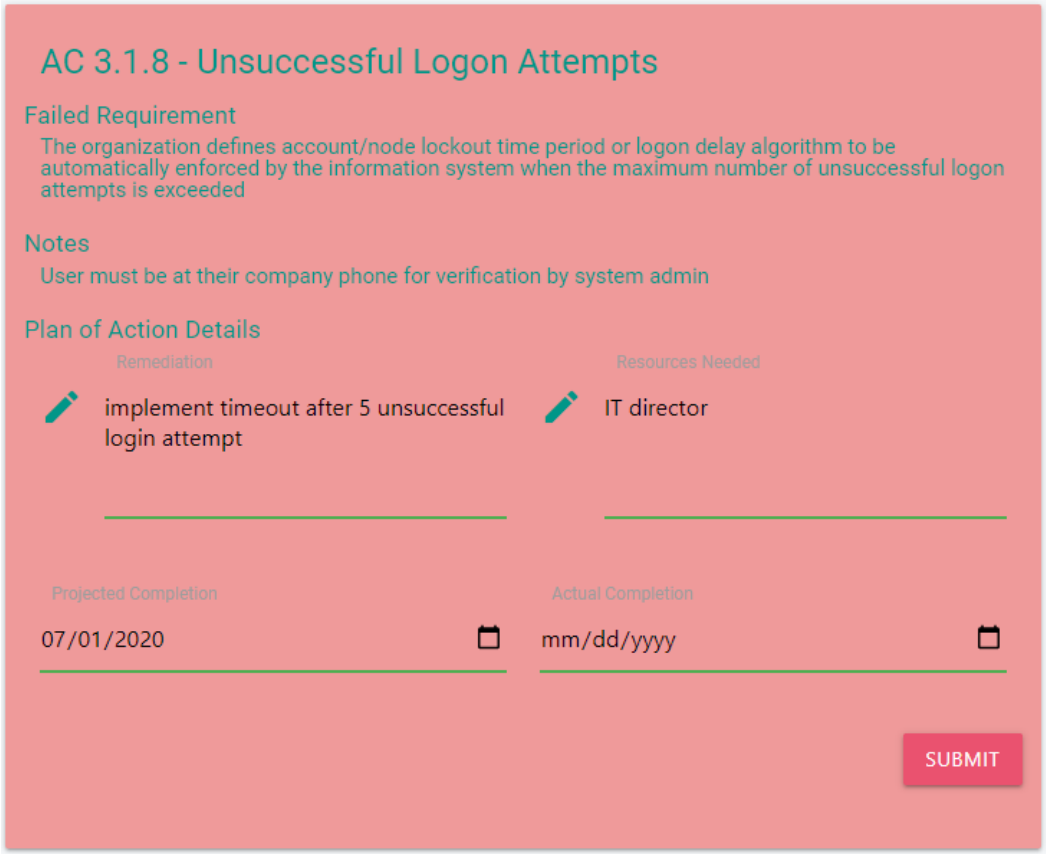
If there were any notes for the control that were entered during control implementation stage (Module 2), they would appear in the notes section on the PO&AM action tile.



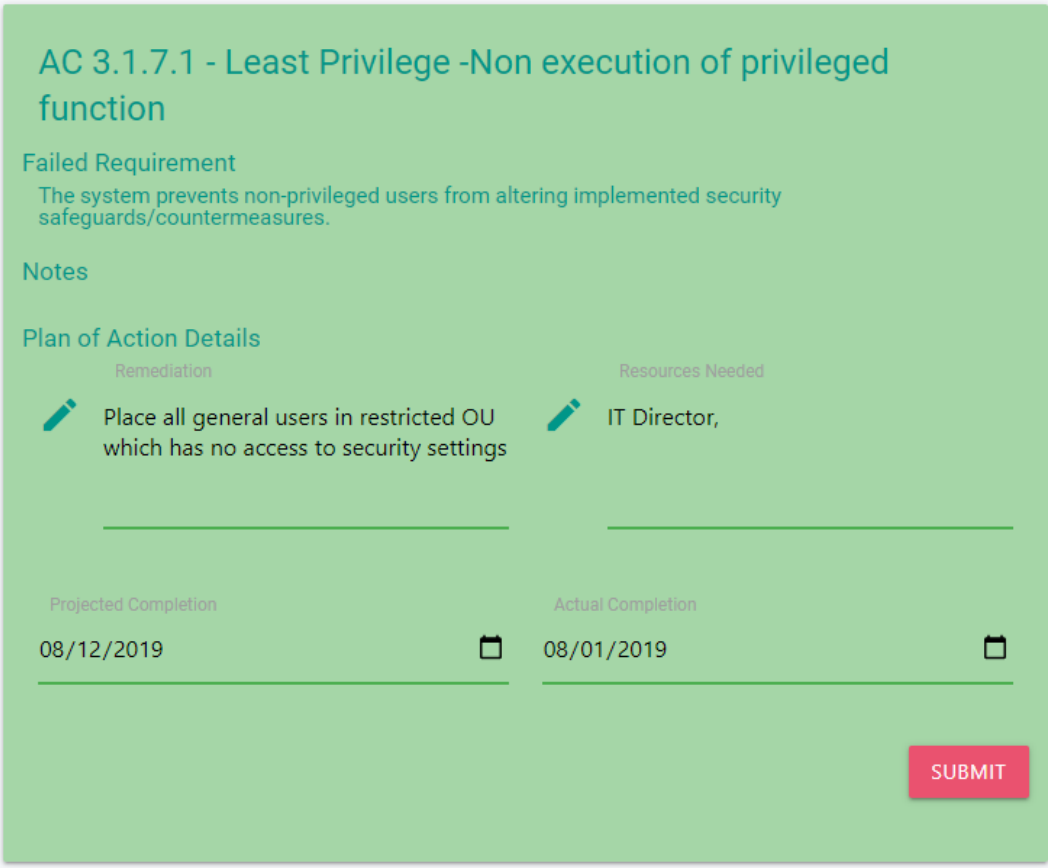
In this example the action was to implement Role Based Access Control (RBAC) for account Management. Note – that notes for this control appear in the POA&M. The ISSO and the IT and operations staff need to decide on the remediation efforts and enter the agreed-upon plan into the appropriate fields. Once the required information is entered, the background color changes to light green. The color will stay light green until either the project is completed (turns dark green) or the completion date has passed without the action being completed (turn red)



Dates can be entered directly or by placing the mouse at the end of the date line. A calendar drop down will appear, and the user can select the desired date.



In this example. the due date was changed to show a time that has already passed. The background color is now red



In this example, the due date was changed, showing the task was completed as indicated by the completion date being entered. The background color turns dark green

The CISO or the executive board is responsible for assuring that POA&M actions receive priority among the many routine IT projects in order to reduce the vulnerability exposure within the agreed-upon timelines.

The POA&M module can be exported to a CSV file at any time by clicking the “Download” button that appears at the top of each screen.

Once the file is downloaded into a CSV file. the POA&M items can be sorted by the following criteria:

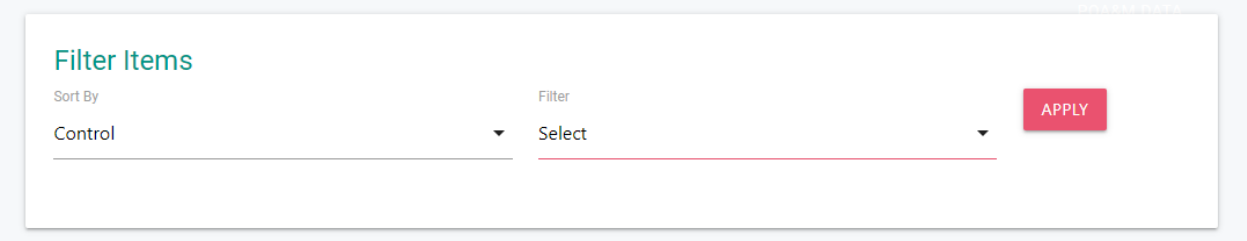
ID Number
Control Domain
Control Number
Control type (basic or derived)
Control Name
Requirement
Status (active or completed)
Remediation
Resources
Projected Due date
Actual Completion date

FILTERS

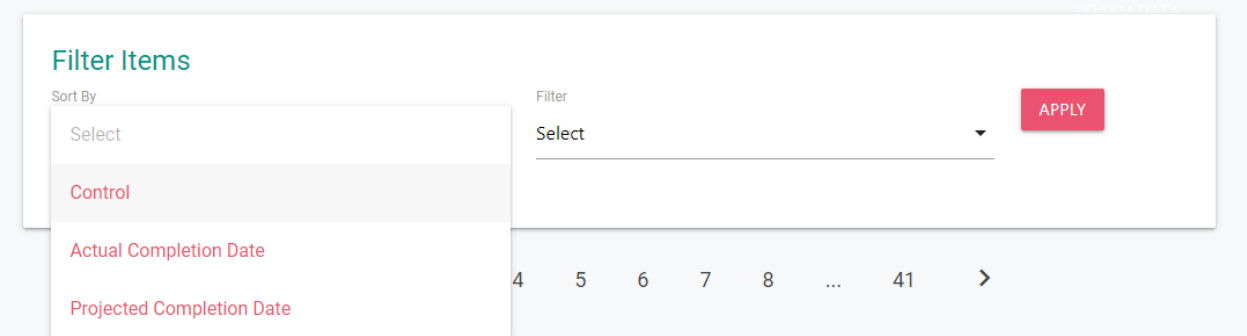
Many organizations will have multiple POA&M items in various stages of completion. ASCERTIS provides several filters to easily sort POA&M items into major groups.

1) Completed POA&M
2) POA&M items that have remediation plans and are on schedule
3) POA&M items that have remediation plans that are overdue
4) POA&M items that have no remediation plan

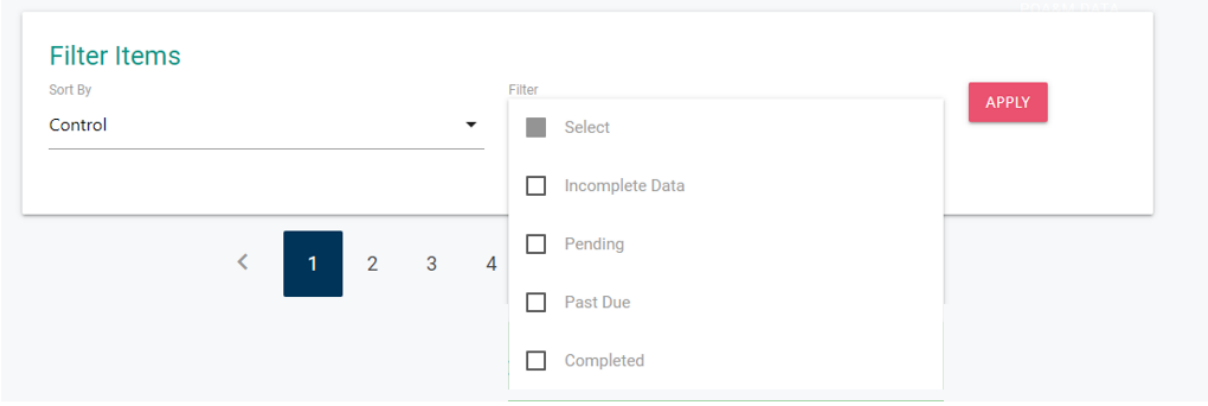
At the top of the POA&M table is the filter bar, see figure below.



The filter bar contains two drop downs. The first drop down allows the user to select a POA&M population to review. The options are 1) All Controls for which there are POA&M items, 2) Controls for which the POA&M items are completed, and 3) Controls for which POA&M items are still being worked.

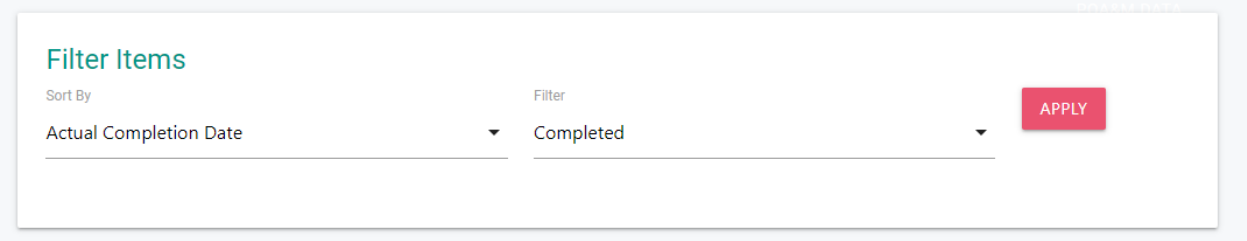


Once the POA&M population is defined, the user can select one or more filters. In the example below the population of POA&M selected, was all "Controls." Therefore the user has the options to 1) Review those POA&M that have not been completed (e.g. no remediation plan has been entered), 2) Review POA&M items that are still on schedule, 3) Review POA&M Items that are past due, or 4) Review POA&M Items that are completed.

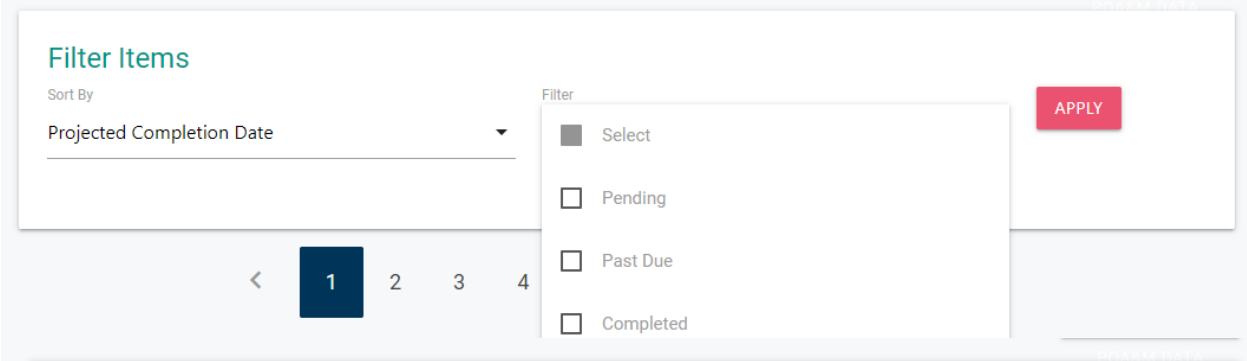


Once the population and filter are selected the user clicks the "Apply" button to activate that sort.

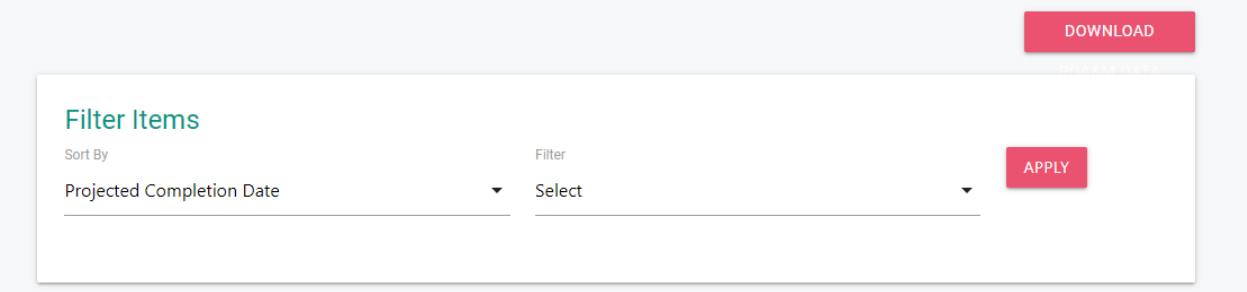
Filtering is context sensitive to the population being requested. For example, if the population is Actual Completion Date, then only the Completed filter is available.



If Projected Completion date is selected, then only the Pending, Past Due, and Completed filters are available.



Filtered sorts can be exported to CSV files using the download button that appears at the top of the filter selection tile.

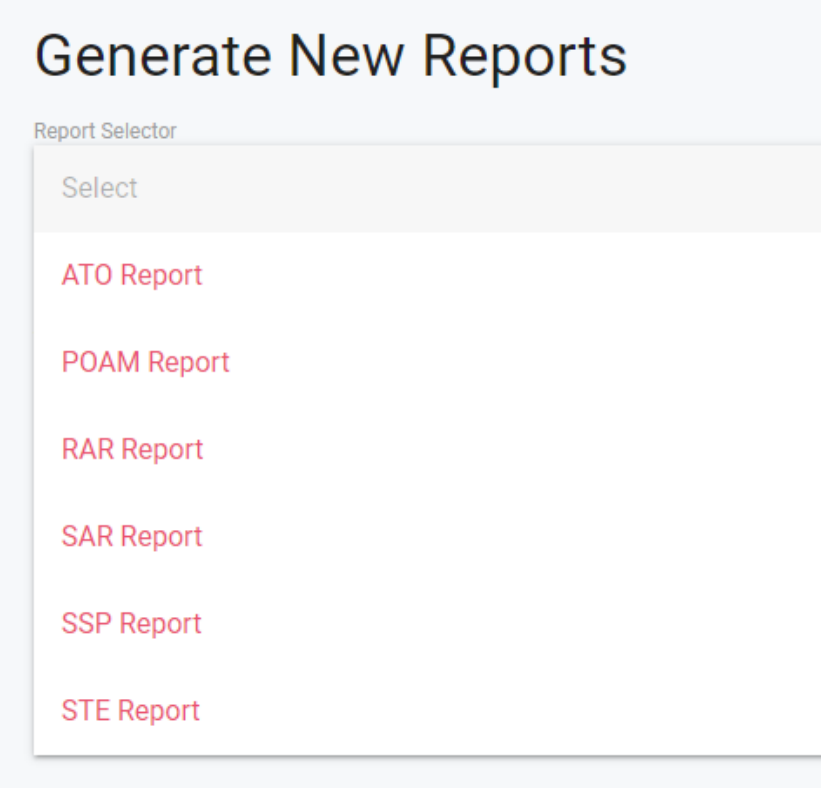


Module 6 – Reports

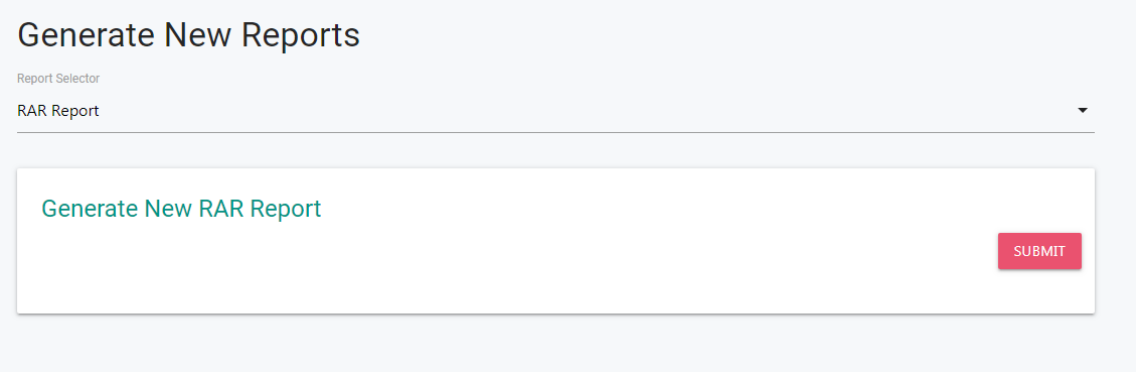
The Government can ask for the bodies of evidence that the Authorizing Official (AO) based this decision on. The Government can terminate a contract if it believes the contractor system was improperly granted an ATO.

ASCERTIS produces the following bodies of evidence reports:

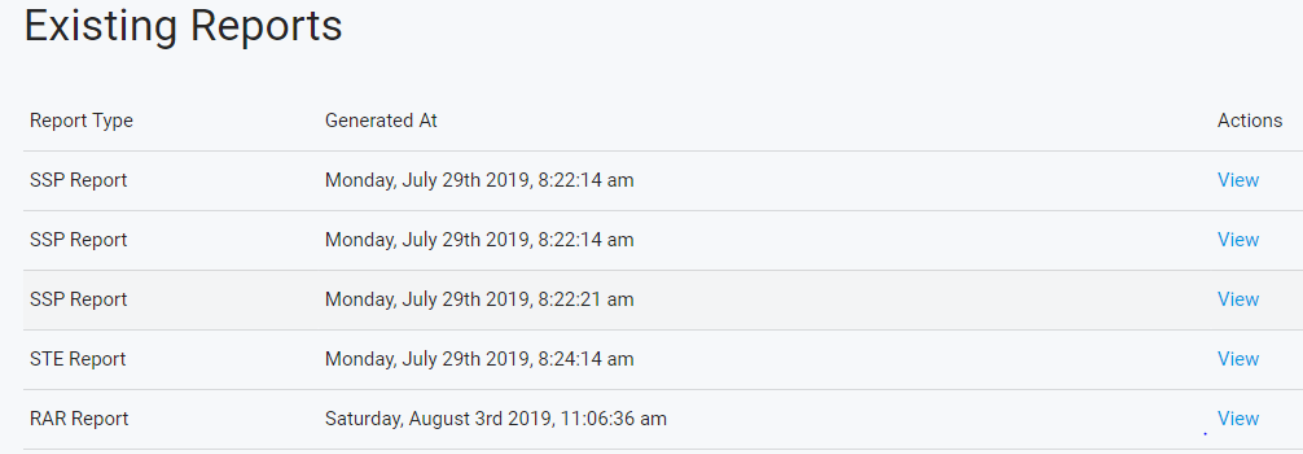
- System Security Plan (SSP)
- Security Test and Evaluation Report (ST&E)
- Security Assessment Report (SAR)
- Risk Assessment Report (RAR)
- Plan of Action and Milestones (POA&M)
- Authorization Letter (ATO)



To generate a report, the user selects “create new report” and then uses the arrow to select the required report.



The reports appear in order of generation requested, with the most current report at the bottom.



The report will appear in the downloads folder in PDF format.

Certification and ATO Letter

The AO must show sufficient documentation to support the authorization decision, as well as to verify the ongoing implementation and operational maintenance of designed security controls. These controls show the AO's intent to provide adequate protection.

The Certifier is an independent reviewer hired by the organization to perform the assessment. The Certifier produces the certification letter. This letter summarizes the overall risk posture of the system, a summary of the most severe POA&M items that need remediation, and a duration that the system can operate pending the remediation of the POA&M items.

The Certifier meets with the ISSO/ISSM or company representative that helped conduct the tests. The ISSO/ISSM is responsible for assuring the POA&M items are completed on schedule. The ISSO/ISSM countersigns the certification letter.

The Certifier then prepares the ATO letter for the AO. The AO is ultimately responsible for the security of the information system and the assurance that the organization will spend the time and money to correct the deficiencies revealed through testing. The AO signs the ATO.

The certification and ATO letter are then uploaded to the ASCERTIS application for future reference and are available via the portal.

The duration of operation is usually three years for low-risk systems. Moderate- and high-risk systems typically have a shorter timeframe for operation, but the timeframe can be extended if the POA&M items are remediated as scheduled. Failure to correct the control deficiencies can result in rescinding the ATO.