Certification Assistant Standard & Premium User Guide

January 2022

Contents

Document Versions

Version	Impacts	Date
Certification Assistant		Pre-June 2021

CA 1.4	1.4 includes:
	• Dashboard redesign
	• Export
	• Printing Updates
	• Update to Individual Self-Assessment:
	    ○ New Tab structure
	        ▪ Controls Comments and Logs (Implementation Statement
	        ▪ Policy References
	        ▪ Assessment guide
	        ▪ Artifact Upload
	        ▪ Action Items
	• Updates to Policies
	• Added Scope to System Description and SPRS report
	• Update SSP/POAM to include approvals to table
		June 2021

CA 1.5	1.5 includes: • All trails now start at Standard level • Multi-factor authentication is not required for a trial • Acceptance of Terms and Conditions inside Certification Assistant for the first user of an organization	August 2021
CA 1.6	1.6 includes: • Ability to upload software and hardware system configurations using standard templates. • Ability to change an Action Item type after it's been created ▪ From NIST to CMMC or BOTH	

	▪ Note: it can only be modified from the control page and not from the Action Item details page
	• Ability to create workflow action items on a scheduled (daily, weekly, monthly, quarterly, yearly) basis
	  ▪ These do NOT change the status of the control
	  ▪ These do show up on the dashboard and the individual control page
	• Improved Navigation
	  ▪ Ability to move to next control within a domain
	  ▪ Ability to quickly decision a control from the domain dashboard page
	• Ability to share links and documents with partners and vs versa
	• Ability to put customers LOGO on the SSP and POAM reports	

![EXOSTAR]

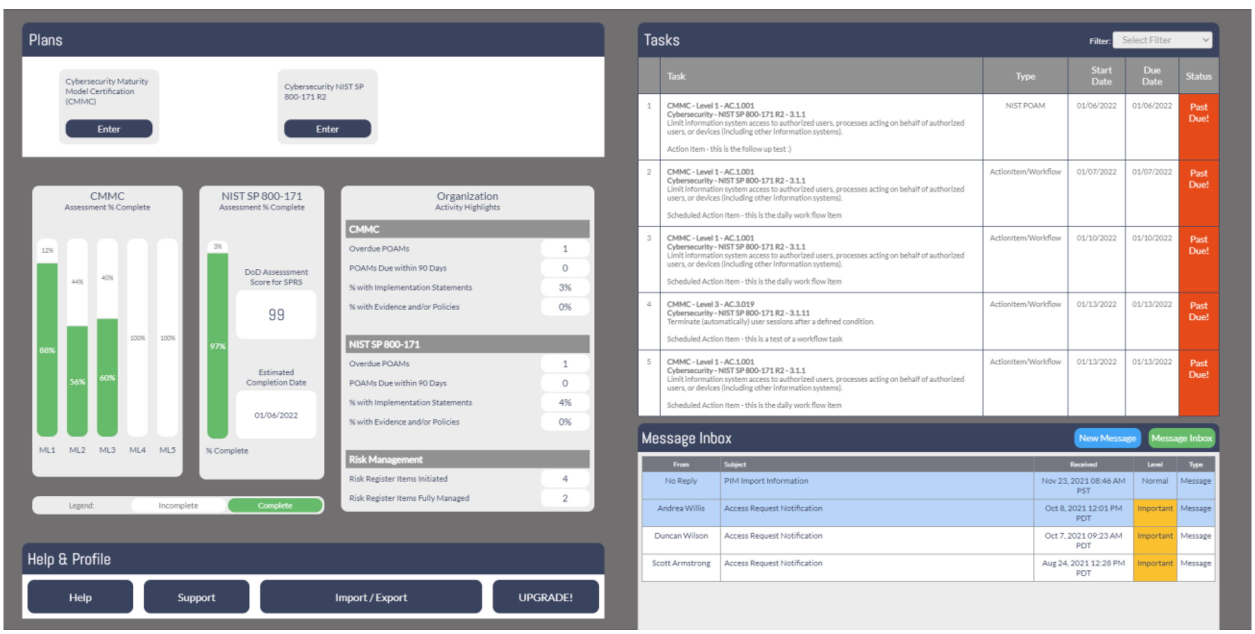
Certification Assistant Standard & Premium Help

All Levels on Standard or Premium have consistent functionality so the Standard version screenshots in this section also pertain to Premium.

Certification Assistant Standard & Premium Home Page

The first page displayed after access Certification Assistant from MAG is the Home Page. The page consists of 5 main sections:

1. Plans – Your currently enabled compliance plans
2. Tasks – Action Items that are currently assigned to the current user
3. Graphs – A high-level snapshot of the progress on controls and action items
4. Message Inbox – Built-in messaging component. Send messages to your team members, clients, or consultants.
5. Help & Profile – Access to help and support resources as well as the button to upgrade your license. Additionally, there is a button to assist you importing your data from PIM if you are a current user of that Exostar application.



To access the CMMC program details, click on the Cybersecurity Maturity Model Certification (CMMC). To access the NIST 800-171 program details, click on the plan link NIST 800-171 R2 link.

To import your PIM data or a previously exported file from Certification Assistant, click on the Import/Export button.

If there are Actions Items available, click on the Task Name to access the task details page.

Import / Export

Certification Assistant provides options to Export your information into two formats, either NIST 800-171 or CMMC. You can Import Certification Assistant data (the same export formats) or use the Exostar Partner Information manager (PIM) data format.

To Export:

Select the desired format from the export drop down list and click on the Export button. An Excel formatted document will be downloaded. You may update the spreadsheet file, but refrain from editing the grey fields, only the yellow fields are editable if you intend to import the file back into Certification Assistant.

> Note: values for the fields are I = Implemented, N = Not Implemented, A = Partially Implemented and E = Not Applicable.

To Import:

Select the format from the import drop down list and click on the Import button. Note: the format selected must match the file format or you will be prompted that you cannot import due to the incorrect format selected. For example: A CMMC export can only be imported as CMMC.

As an existing Exostar PIM user, you can export your existing data and import into Certification Assistant.

Access PIM and perform an export of your existing data. This should produce a .csv file for use by Certification Assistant to import. Refer to PIM user help for details on exporting.

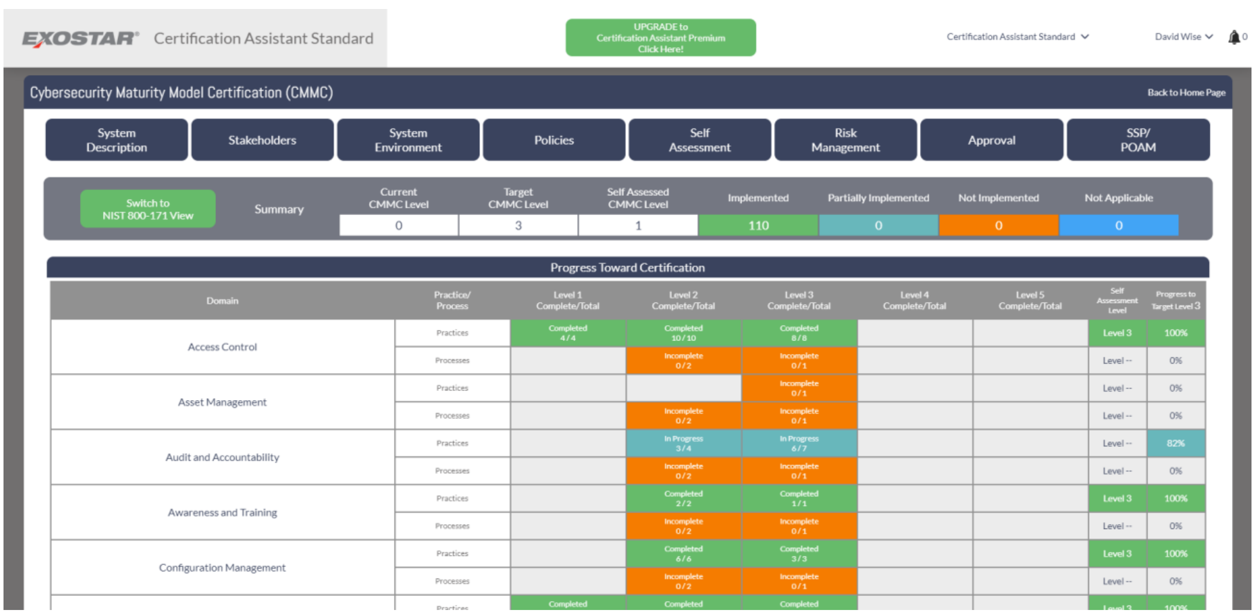
Select the Exostar Partner Information Manager option from the import drop down. Select your .csv file and click on the Import button.

On Import, you have the option to have the existing Certification Assistant date updated or replaced. Select the desired radio button and then import the file. Note: all uploaded documentation artifacts, implementation statements and action items will be preserved regardless of status update choice.

> Note: values for the fields are I = Implemented, N = Not Implemented, A = Partially Implemented and E = Not Applicable.

Home Pages – both CMMC and NIST 800-171

The CMMC home page contains the detailed resources to update your status on CMMC Certification.



The Tab Toolbar is how you will navigate through the system to complete each section.

The Summary bar shows your current CMMC Level, Target CMMC Level, Self-Assessed CMMC Level and the number of controls in each level of implementation: Implemented, Partially Implemented, Not Implemented, and Not Applicable.

Summary	Current CMMC Level	Target CMMC Level	Implemented	Partially Implemented	Not Implemented	Not Applicable
	0	3	35	30	43	2

The Progress Toward Certification table gives a complete progress in each CMMC domain toward your goal certification level.

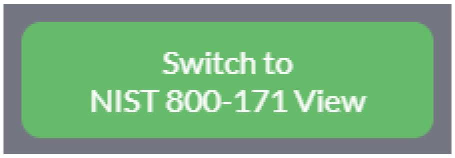
Progress Toward Certification

Domain	Practice/ Process	Level 1 Complete/Total	Level 2 Complete/Total	Level 3 Complete/Total	Level 4 Complete/Total	Level 5 Complete/Total	Self Assessment Level	Progress to Target Level 3
Access Control	Practices	In Progress 2 / 4	In Progress 5 / 10	In Progress 2 / 8			Level --	41%
	Processes		Incomplete 0 / 2	Incomplete 0 / 1			Level --	0%
Asset Management	Practices			Incomplete 0 / 1			Level --	0%
	Processes		Incomplete 0 / 2	Incomplete 0 / 1			Level --	0%
Audit and Accountability	Practices		In Progress 1 / 4				Level --	25%
	Processes		Incomplete 0 / 2				Level --	0%

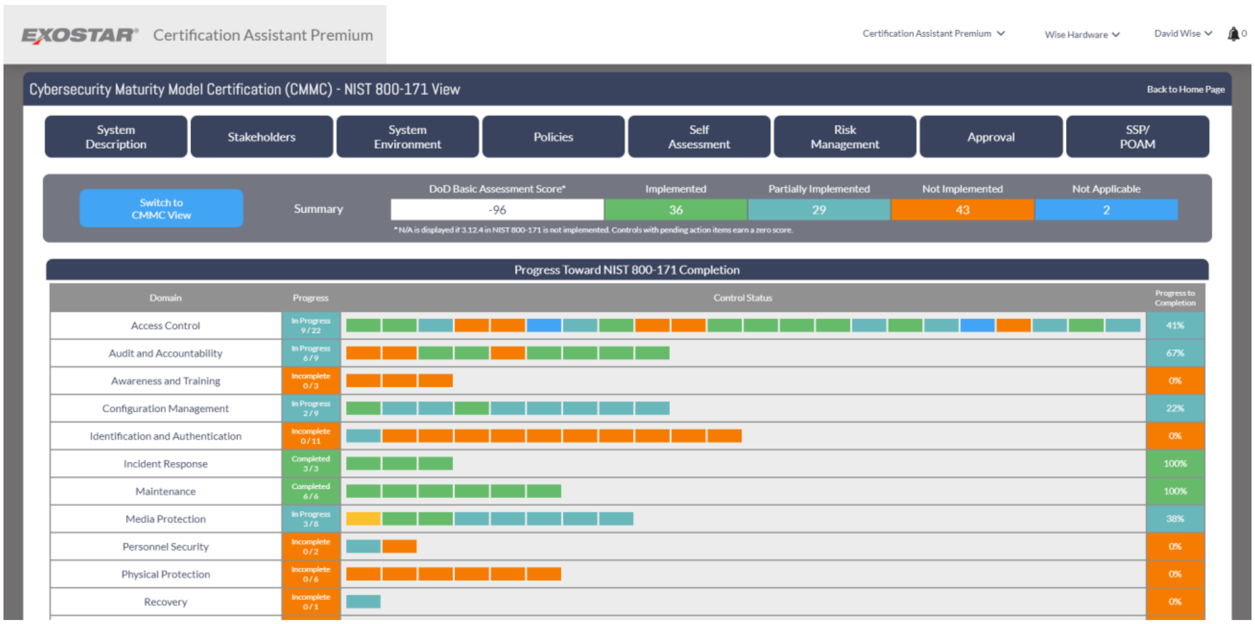
How to read the chart:

- There are Practices and Processes in each CMMC domain from Level 2 on, except for Access Control.
  - There are limited practices and no processes in Level 1, therefore the chart shows a grey cell with no data.
  - Similarly, this instance is only subscribed to Certification Assistant Standard, so Level 4 & 5 are also grey.
- When a Level contains 0 completed controls, it will show orange and 0 out of 2 (for example) Incomplete.
- When a Level contains between 1 and the full number of controls, the cell will show lite blue and show In Progress.
- When a Level has all controls completed, the cell will show green and be labeled Complete.
- When a Level is complete, the 'Self-Assessment Level' column will show the highest level currently completed.
- The Progress to Target Level 'X' column will show a percentage of progress toward the goal.
- Each cell on the chart with progress data is also clickable and will navigate you directly to the selected Level and Domain.

Click on the Switch to NIST 800-171 View button to change the Home Page to NIST 800-171 and the progress on that Plan.



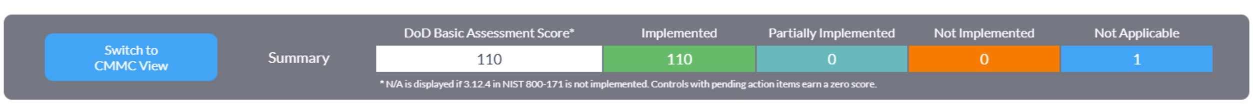
This is the NIST 800-171 Home Page. This is accessed by either the green button the CMMC Home Page or by the Dashboard Plan link.



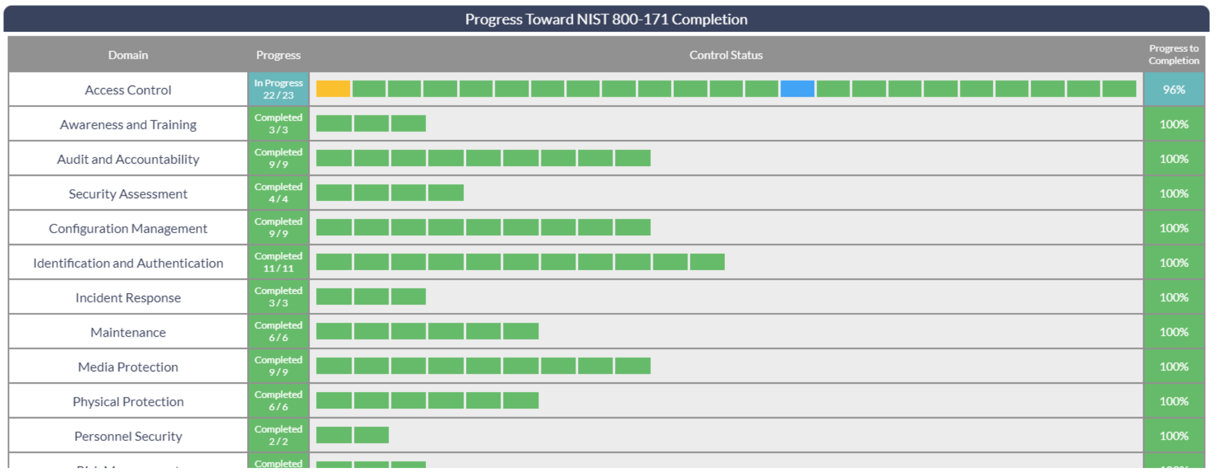
Similar to the CMMC Dashboard, the Tab Toolbar is how you navigate through the detailed information.

The Summary bar gives you the status information against NIST 800-171. DoD Basic Assessment Score is the score for SPRS and each control triggers points in the score. It will automatically be updated as you work through and status the controls. The other summary items show the status and progression through the controls.

Click on the Switch to CMMC View to return to the CMMC Home Page.



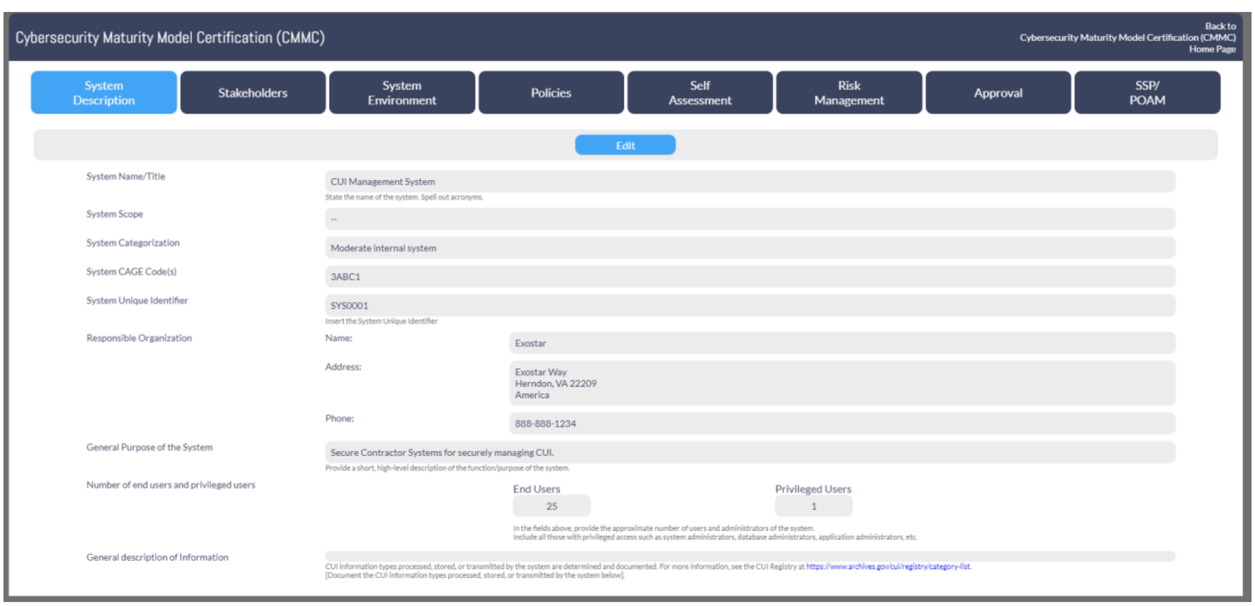
Each of the colored blocks represent a specific control within each domain. The color coding is the same as CMMC. Click on the block to navigate directly to the control. The far right column shows Progress to Completion for all the controls within a single Domain.



All the Tabs described here are in BOTH CMMC and NIST 800-171.

System Description Tab

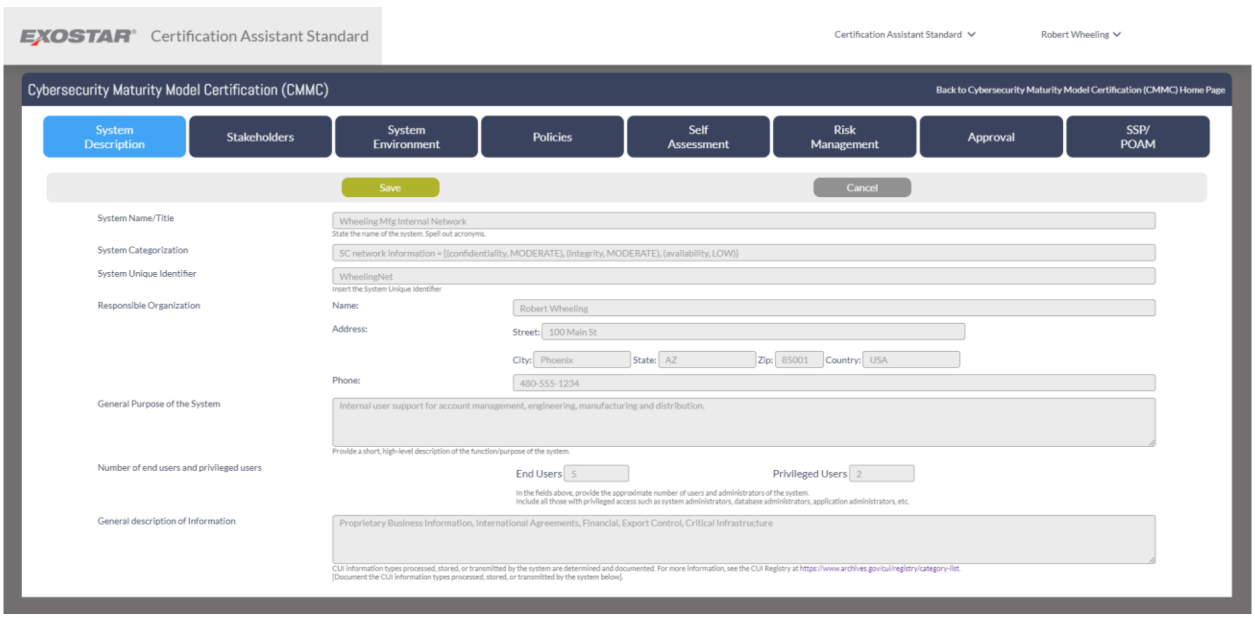
The System Description tab is used to start the information gathering required for a System Security Plan or SSP report. Click on the 'Edit' button to enter edit mode and complete the form.



Enter the information in each field and click on the Save button when complete.

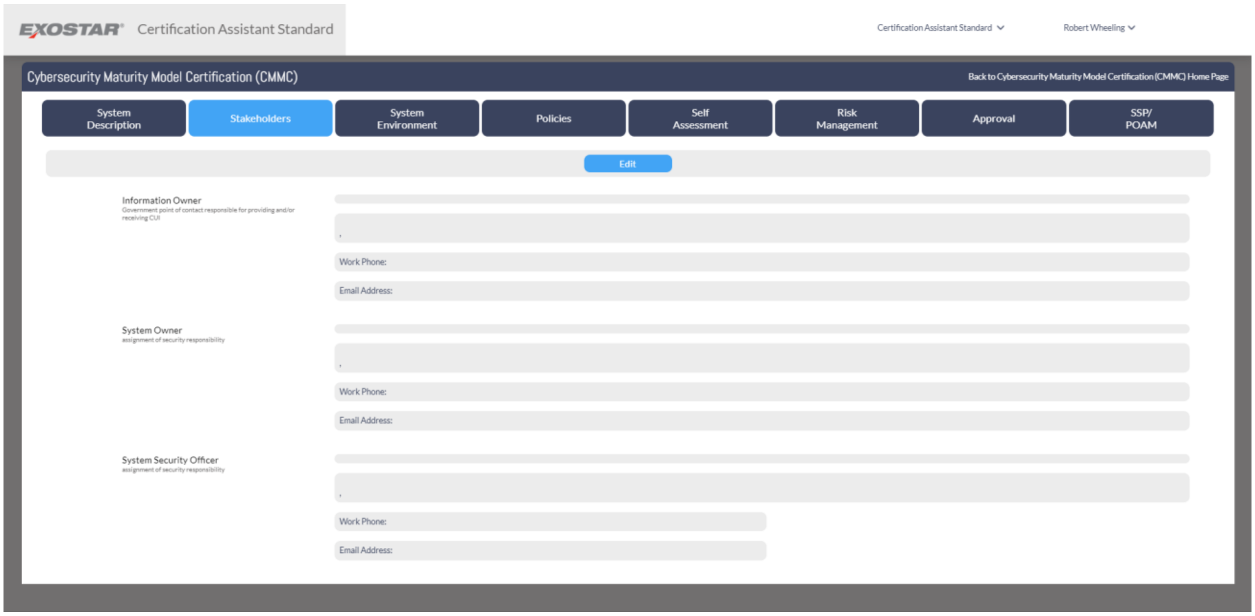
Notes regarding a selection of the fields:

- System Categorization: In general, the format for this field is
  - SC for Security Category
  - The information type – example ‘information system’ or ‘contract system’
  - A High/Moderate/Low impact rating for confidentiality
  - A High/Moderate/Low impact rating for integrity
  - A High/Moderate/Low impact rating for availability
  - Together in this format:
    - SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}
- General description of information – use the link provided under the text box to view a list of CUI information types.

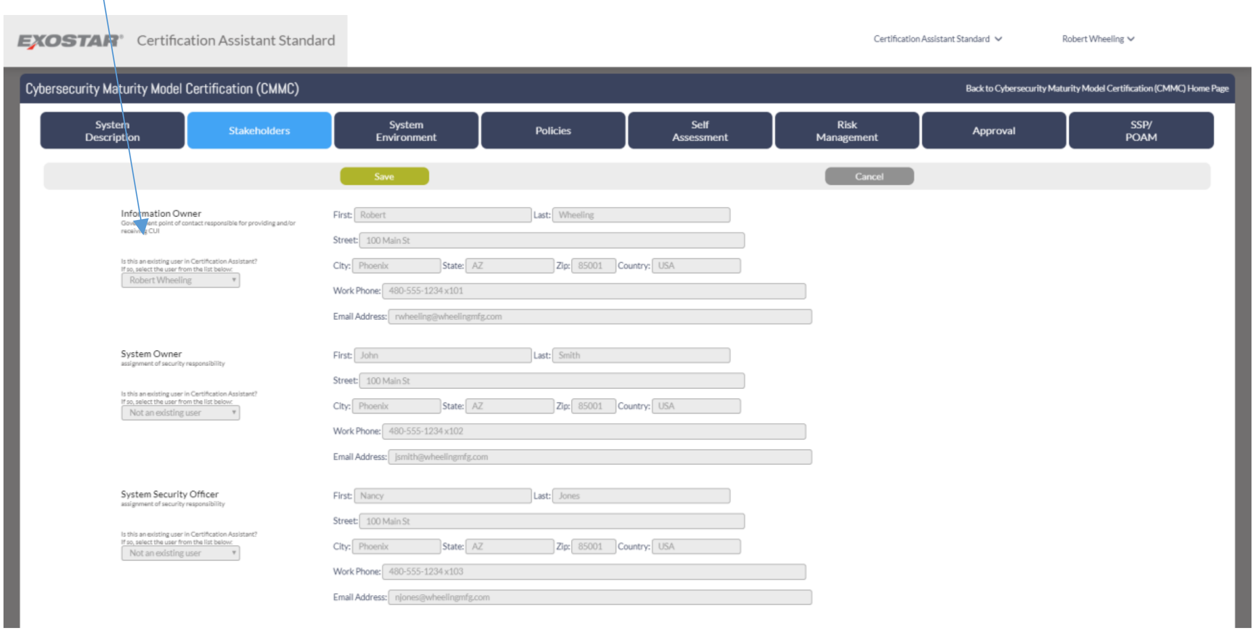


Stakeholders Tab

The Stakeholders tab is where you will identify the Information Owner, System Owner and System Security Officer for this organization. Click on the Edit button to access edit mode and update the information.



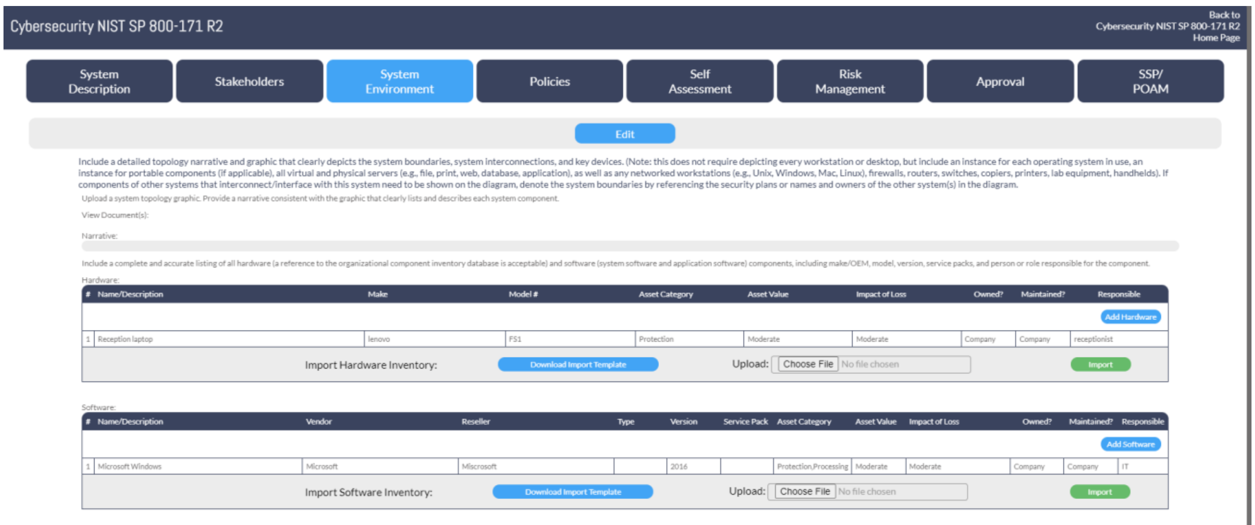
If the any of the individuals are also users of Certification Assistant, use the drop-down list to select their name and enable online electronic signatures in the Approval tab. Note the individual does not need to be a Certification Assistant user.



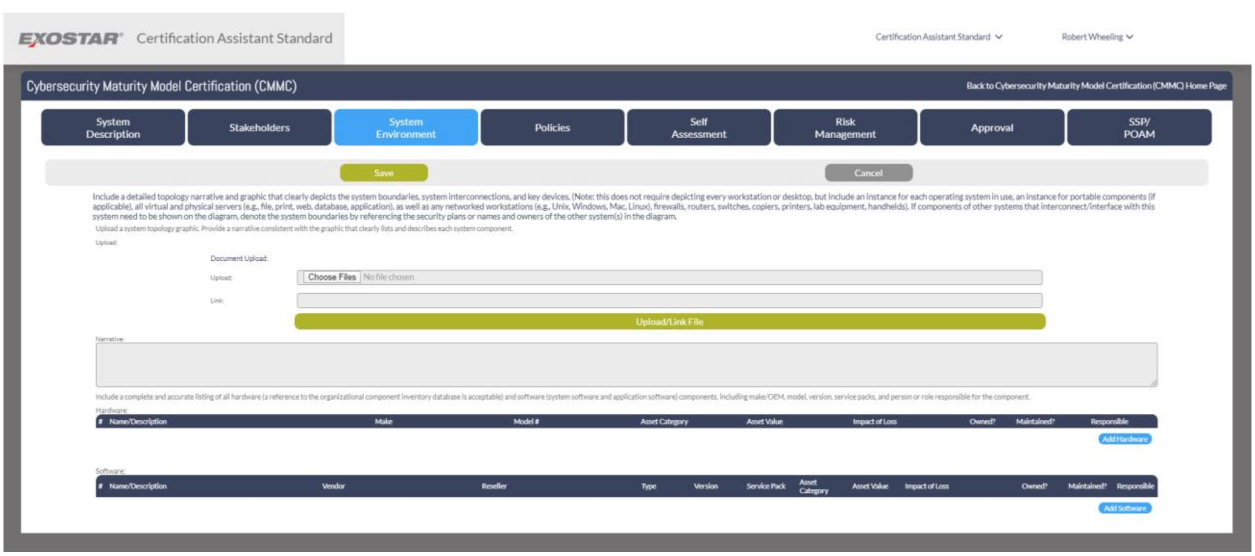
Click on the save button when editing is completed.

System Environment Tab

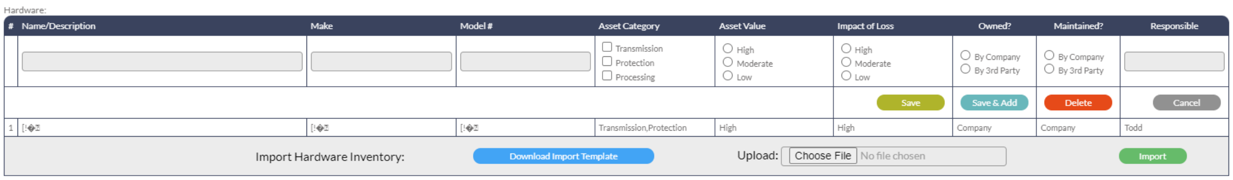
The System Environment tab is for the detailed documentation of the system. Click on the Edit button to open the top portion of the screen for edit.



Upload a detailed topology diagram and enter a narrative to support the graphic in the fields provided. You may upload file(s) or link(s) to externally available files using the Link field. If a document needs to be replaced, use the delete 'X' to remove the document and upload the revised version.

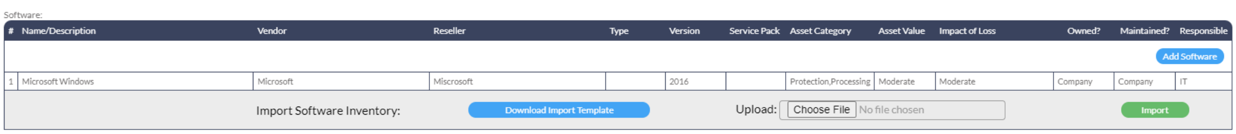


To list your Hardware inventory, click on the Add Hardware button. This will open the form for adding new hardware to the list. The following fields need to be entered: Name/Description, Make, Model #, Responsible and then select from the available values for Asset Category, Asset Value, Impact of Loss (relates to Risk Management), owner and maintenance for the inventory asset.

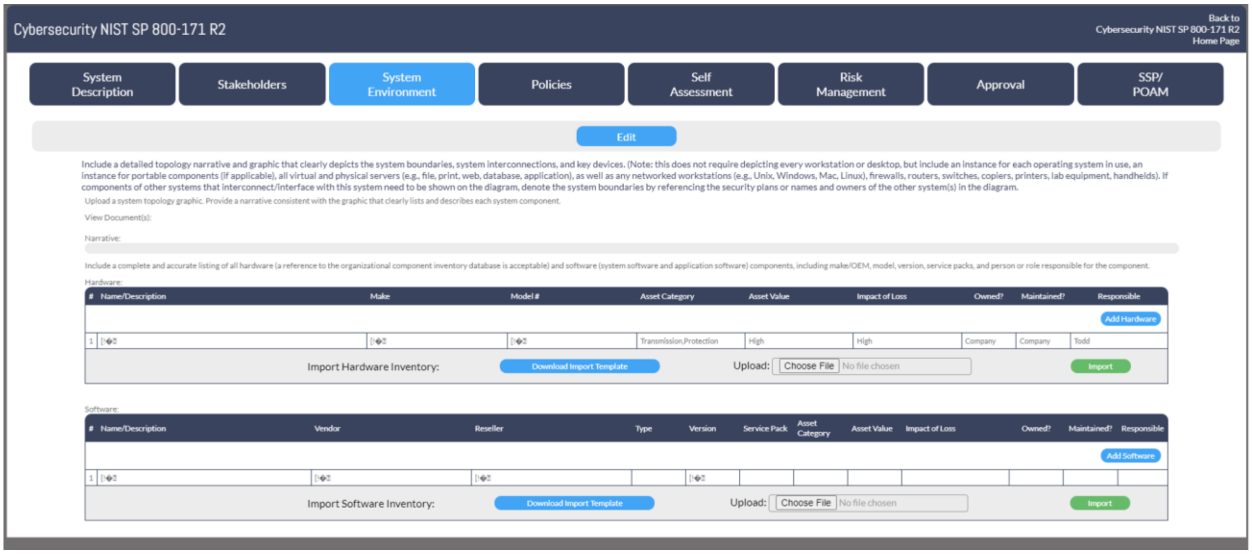


Note: Asset Category defines how this asset is used relative to CUI – is it for the Transmission, Processing, and/or Protection of CUI.

To list your Software Inventory, use the Add Software button. This will open the form to add software to the list. The following fields will need to be entered: Name/Description, Vendor, Reseller, Type, Version, Service Pack, Responsible, and then select from the options for Asset Category, Asset Value, Impact of Loss (related to Risk Management), Owned, and Maintained for the software.

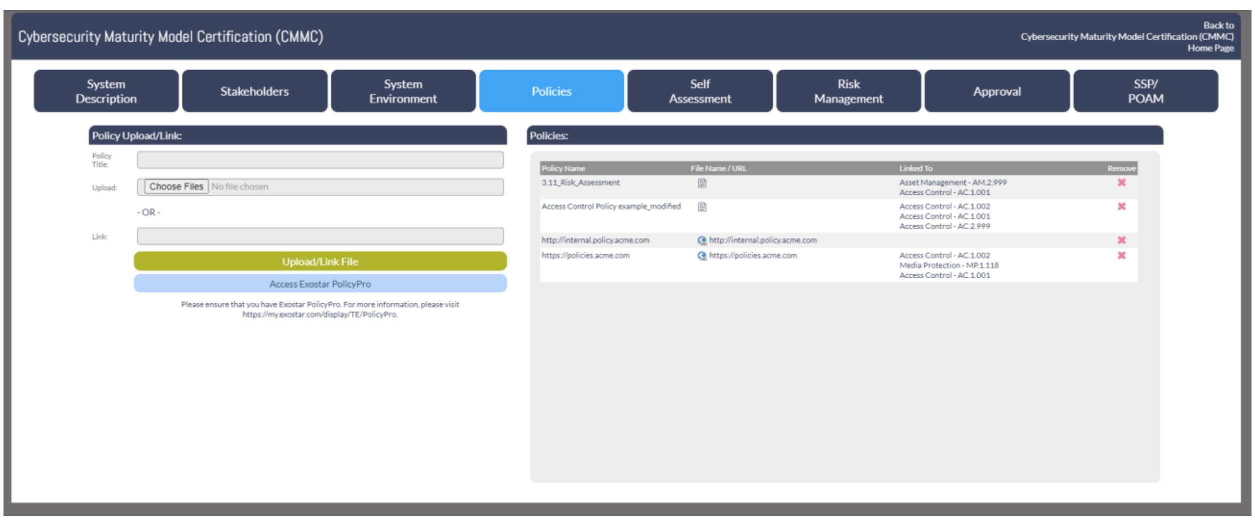


You also can now upload your Hardware and Software Inventory. The template needed is on the bottom of tables. The required values are in the template on the far right. Simple fill it out, save it as a file on your computer (with the same file extension i.e. do not change it), and then upload.   Once you've chosen the file, click Import.

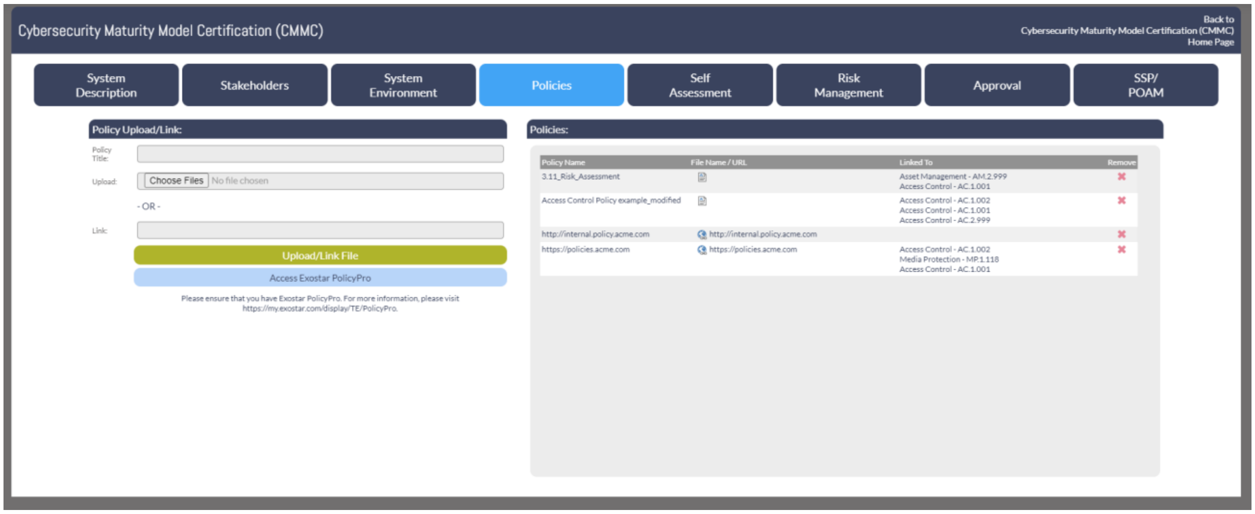


Policies Tab

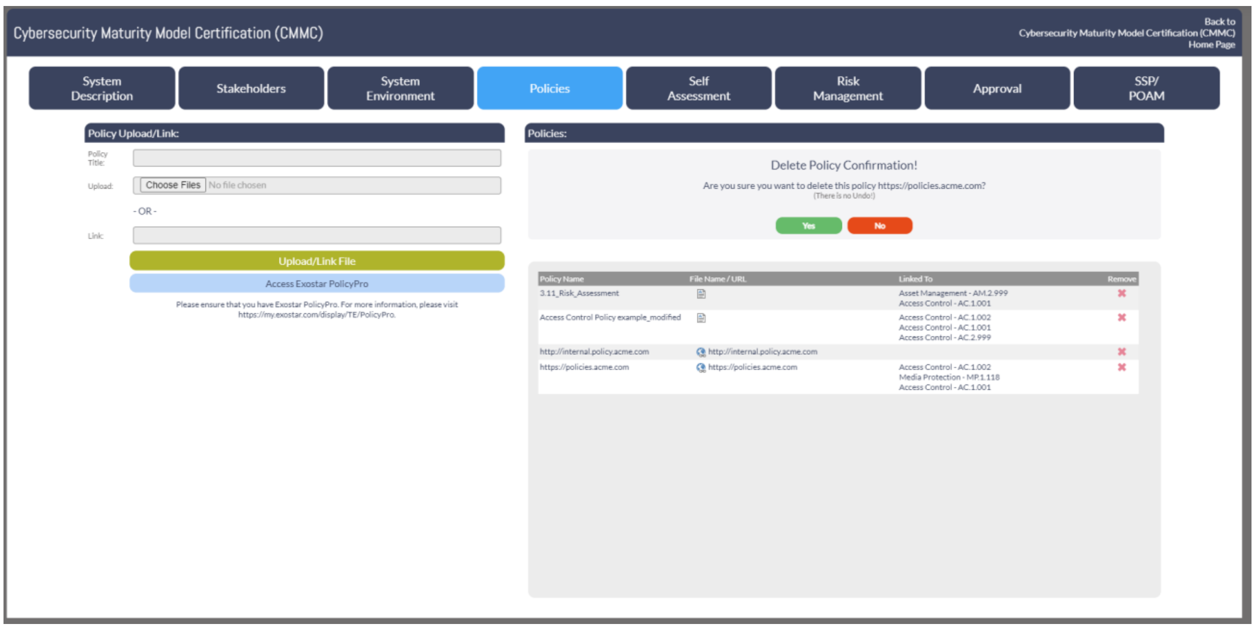
The Policies tab is used as a repository for all policy documentation referred to in the controls. Click on the button to choose your files – multiple files can be uploaded at the same time. You can add the link to Certification Assistant for files that are stored and available externally. Use the blue Open Exostar PolicyPro to access PolicyPro and your content.



Once your files are uploaded, they can be removed using the delete 'X'.



You will have the option to confirm the file removal before it is completed.



Self-Assessment Tab

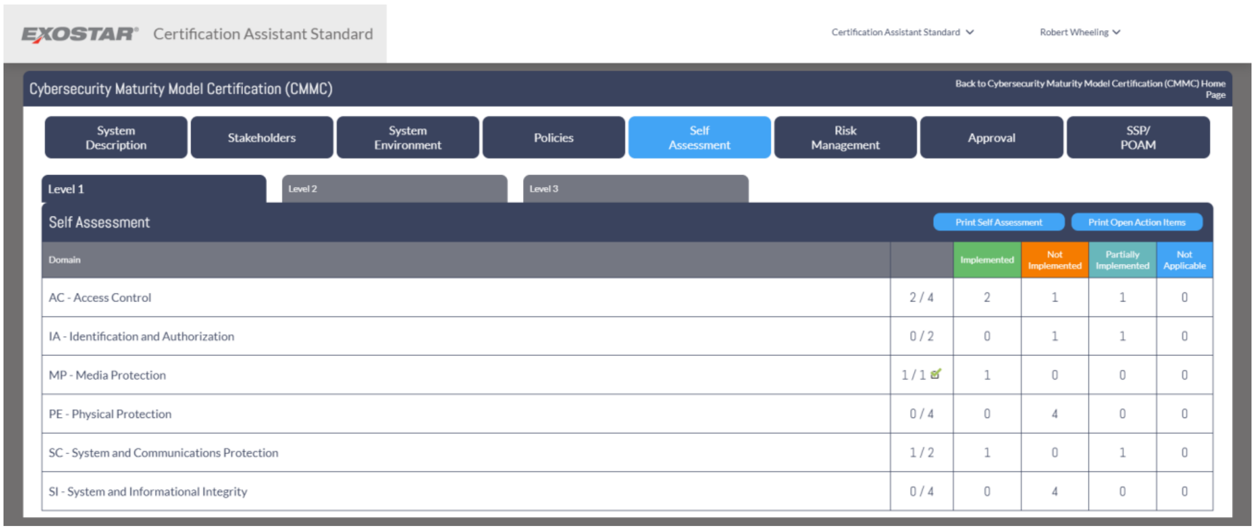
The Self-Assessment tab is where the CMMC Levels with Practices and Processes or the NIST 800-171 Controls are held. Certification Assistant Lite is limited to Level 1, Standard adds Level 2 & 3 and NIST 800-171, and Premium adds Level 4 & 5.

This tab has 2 sections:

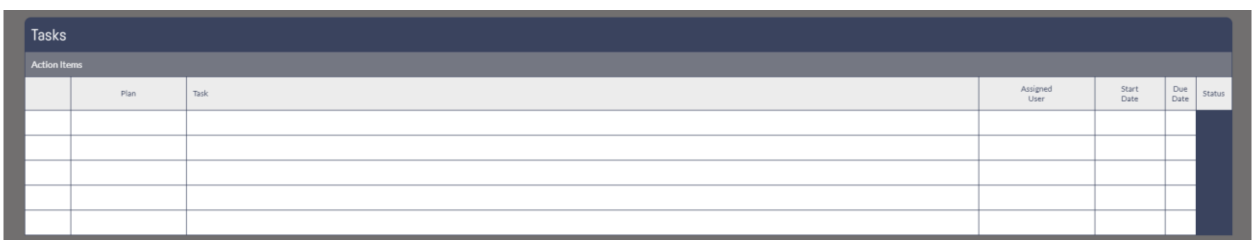
Upper section is a list of the Domains available in the Level with the status for each domain.

Lower section is all open Action Items for the CMMC or NIST 800-171 program.

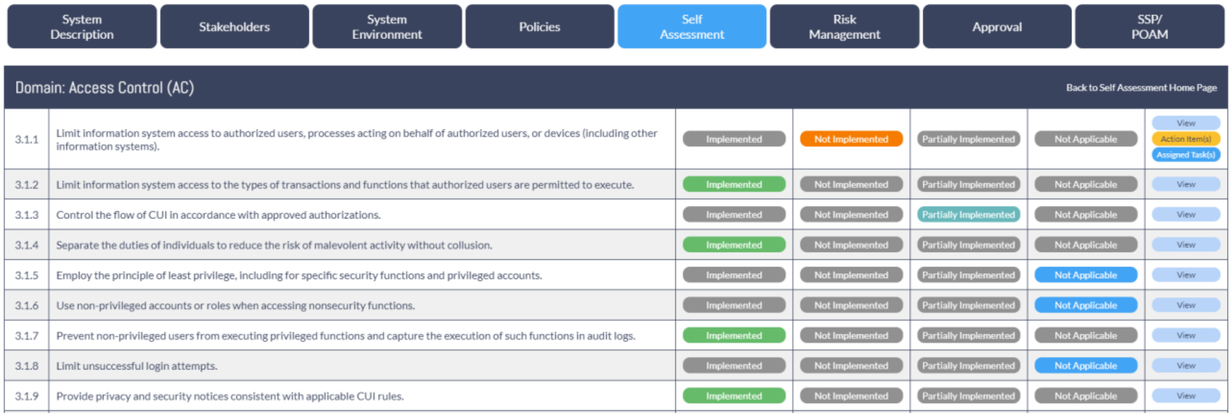
You have the ability from this screen to print out the Self-Assessment and the Open Action Items.



Domain		Implemented	Not Implemented	Partially Implemented	Not Applicable
AC - Access Control	2 / 4	2	1	1	0
IA - Identification and Authorization	0 / 2	0	1	1	0
MP - Media Protection	1 / 1	1	0	0	0
PE - Physical Protection	0 / 4	0	4	0	0
SC - System and Communications Protection	1 / 2	1	0	1	0
SI - System and Informational Integrity	0 / 4	0	4	0	0

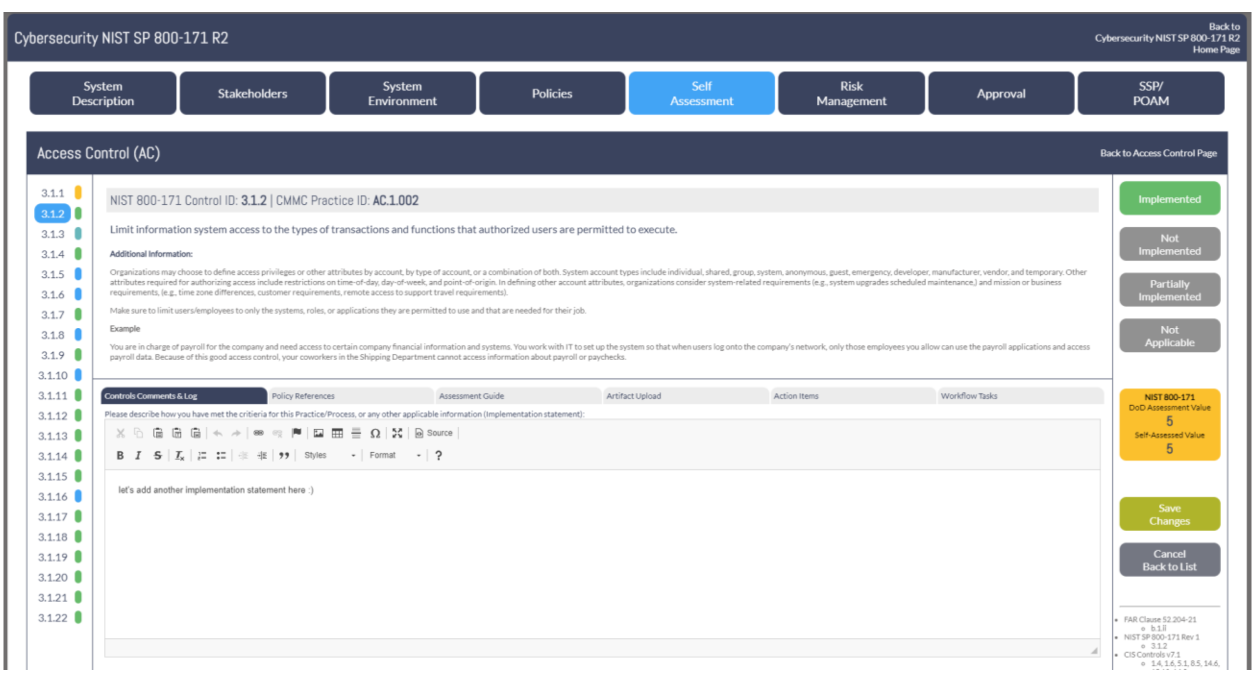


Click on a Domain name (Access Control in this example) and the Practices within that domain are displayed. Click on the View button or click on the practice brief description to view the control details. You now also can decision an individual control from this page. Please remember though that any status does require an implementation statement and potentially artifacts that can only be added from within the individual control.

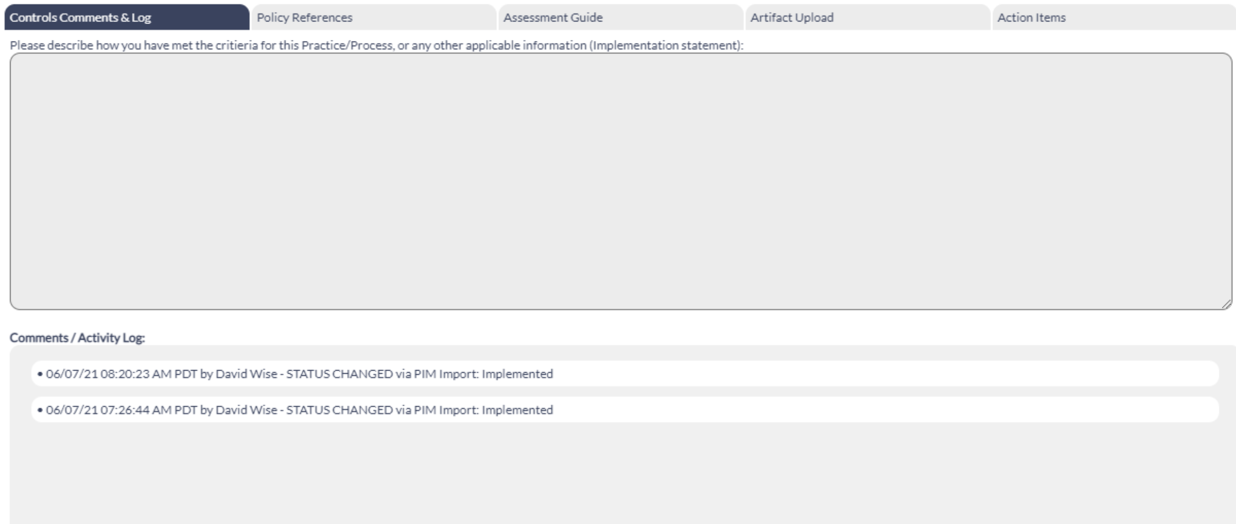


The Control Detail page has 3 main components:

1. The Left side panel shows all possible controls for the Domain and allows for easy navigation by clicking on the control number.
2. The center panel show the Practice content and Additional Information to assist you implementing the control. Below the Additional Information there are now tabs for other items like artifacts, policies, implementation statements and CMMC Assessment Guide documentation.
3. The right panel holds the action buttons and reference information. Each status button can be clicked to change the control to that status and any status changes are automatically saved. Any changes to the other content will require the user clicking the Save button. Use the Cancel or Back to List button to return to the control list. The bottom right has the reference material related to each individual control.



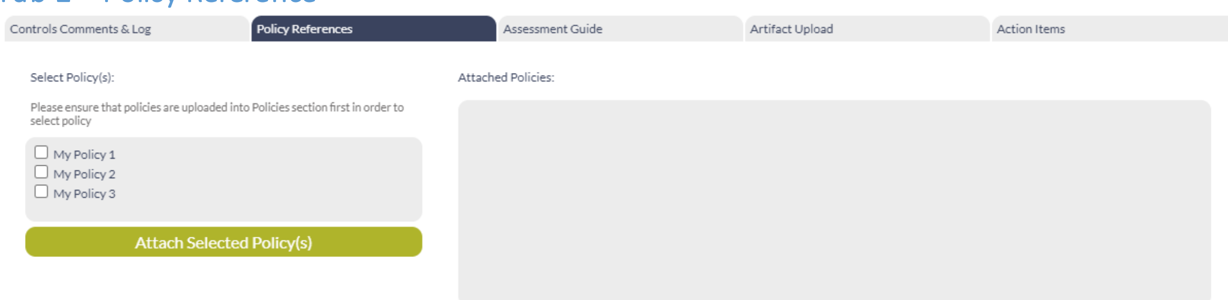
Tab 1 – Controls Comments & Log



The large text box is used to enter your Implementation Statement regarding the control. If you make edits to the statement, the original version of the statement will be added to the Comments/Activity Log. Content in the main text box will be included on reports and the SSP document.

Note: All other interactions with the control such as status changes, will be entered in the Comments/Activity Log.

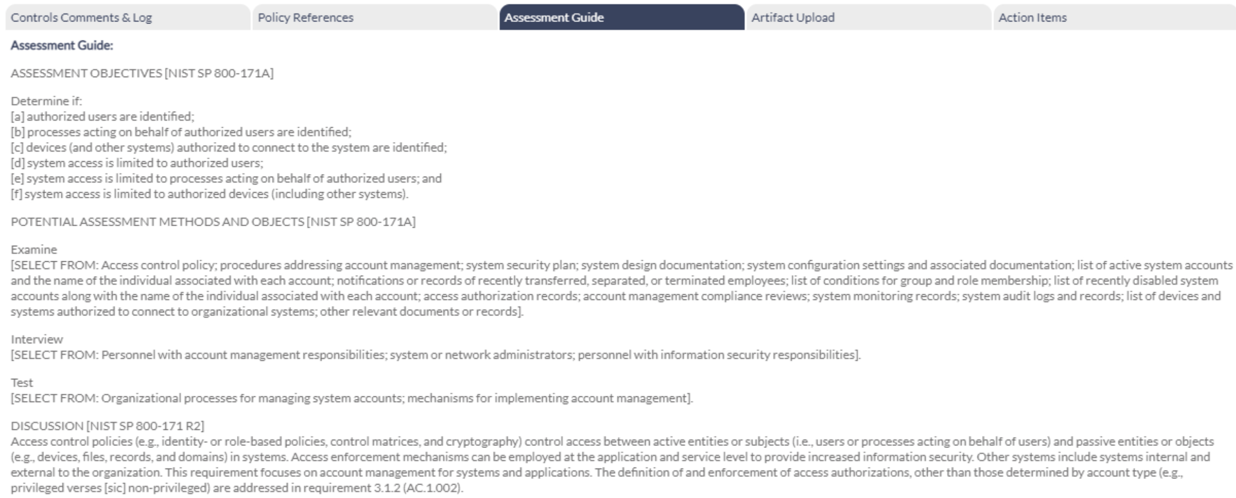
Tab 2 – Policy Reference



You will need to upload all the organizations policies through the Policy Tab then they will be here listed to be selected. Note: only those policies NOT already assigned will be available to associate.

Select Policy(s) to be linked to this control. Use the red 'X' icon to remove a policy link. The document will not be affected by removing the link.

Tab 3 – Assessment Guide


Controls Comments & Log | Policy References | Assessment Guide | Artifact Upload | Action Items

Assessment Guide:

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:
[a] authorized users are identified;
[b] processes acting on behalf of authorized users are identified;
[c] devices (and other systems) authorized to connect to the system are identified;
[d] system access is limited to authorized users;
[e] system access is limited to processes acting on behalf of authorized users; and
[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine
[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

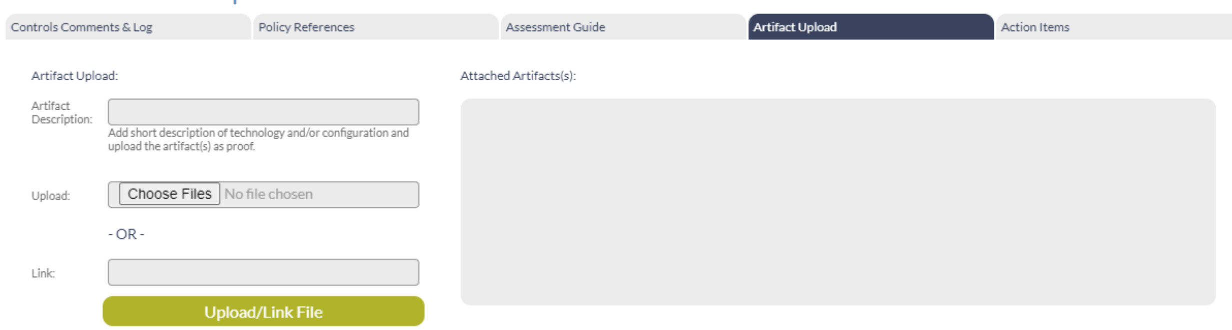
Interview
[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test
[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

DISCUSSION [NIST SP 800-171 R2]
Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses [sic] non-privileged) are addressed in requirement 3.1.2 (AC.1.002).

For additional guidance will completing the controls, the CMMC Assessment Guide has been added for your reference.

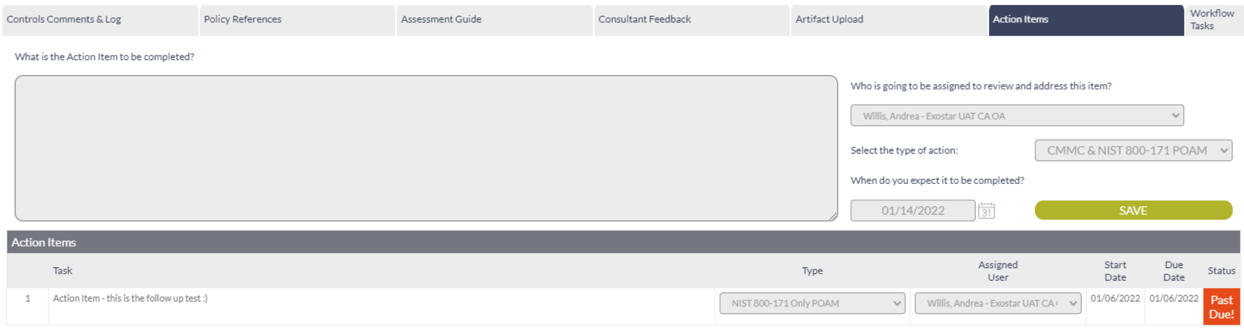
Tab 4 – Artifact Upload



To upload document artifacts specifically for this control, enter an artifact description and choose a file to upload. Use the red 'X' icon to remove an artifact if needed.

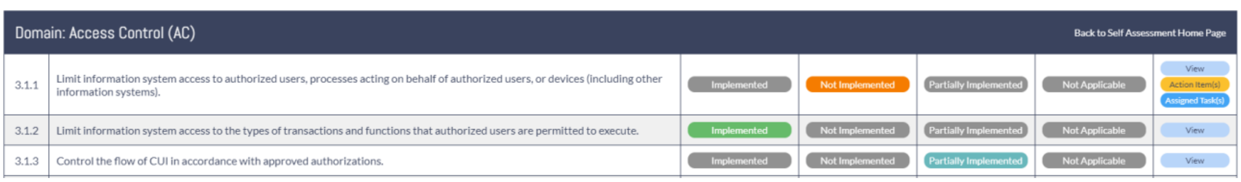
Note: Any artifact that applies to more than 1 Control will need to be uploaded to each individual control.

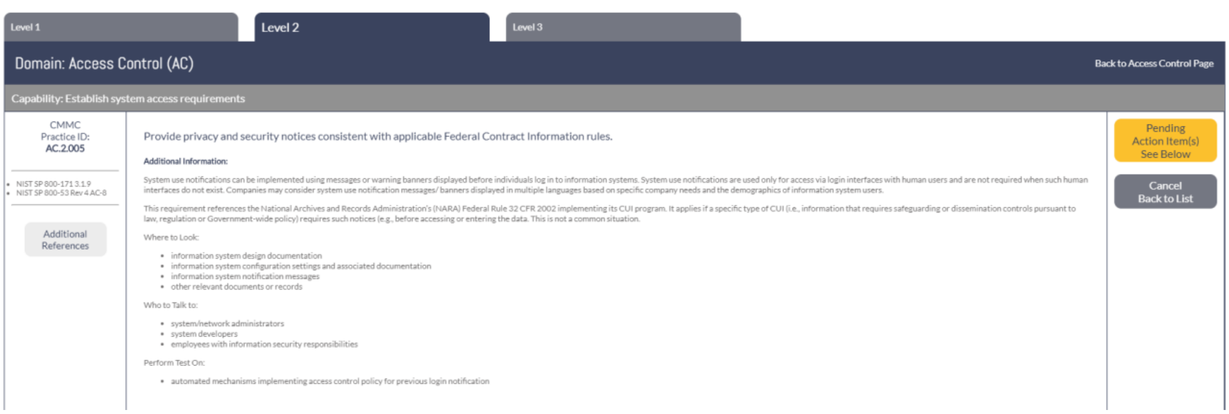
Tab 5 – Action Items



Action Items for a control are managed on the Action Items tab. This is also how you add them in the Action Items tab. Select the user to be assigned the item, identify the item as CMMC POAM, NIST 800-171 POAM, or Both, set a due date and click on Save. The user assigned will receive an email notifying them of the task assignment. You can now update the Type after the action item has been created.

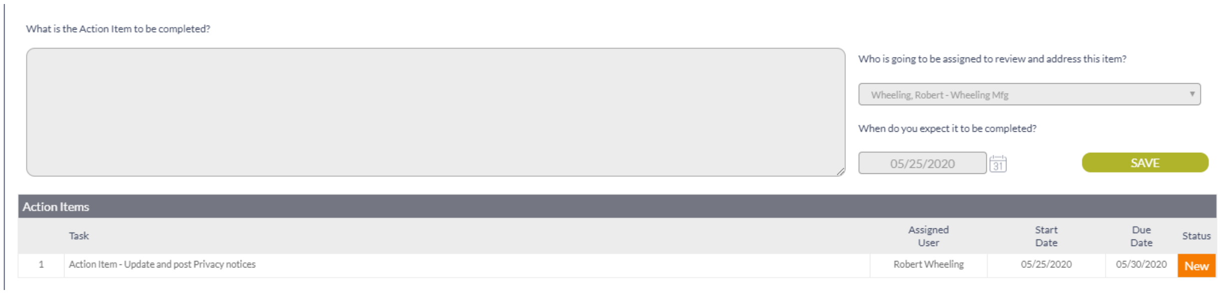
While a control has an open Action Item, the Status icon on the list will show 'Action Item' and in the control details, the button 'Pending Action Item, See Below' is shown. Also the Self-Assessment tab will have a yellow square or icon





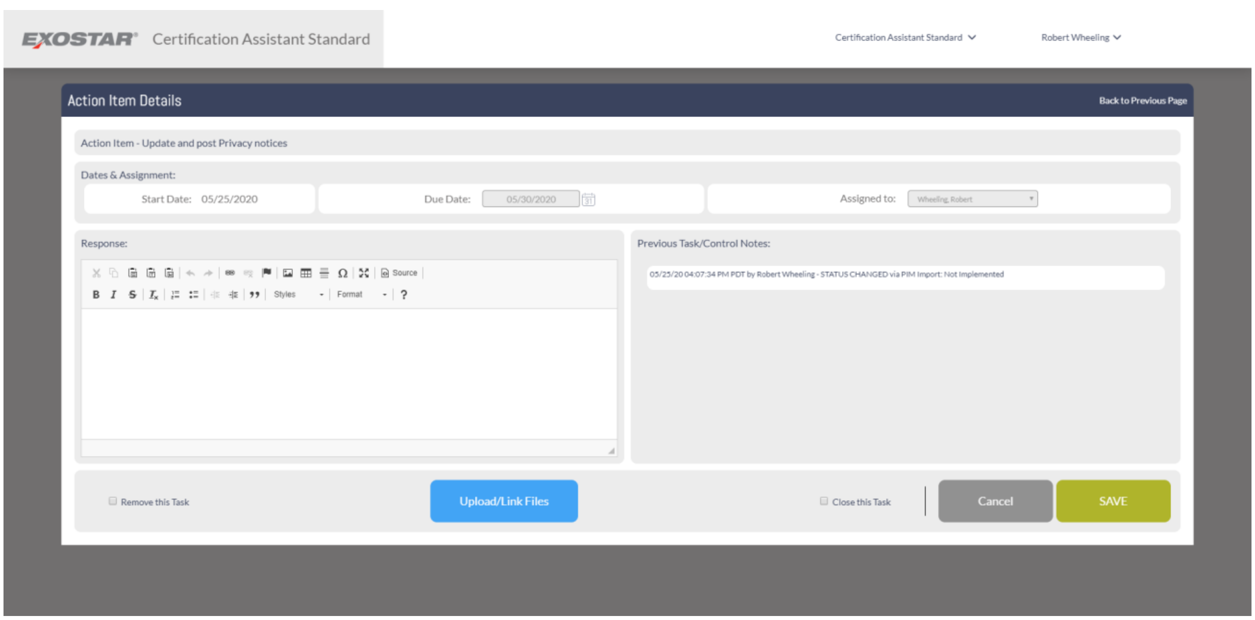
Clicking the pending action button will snap down to the open Actions for the control.

EXOSTAR®

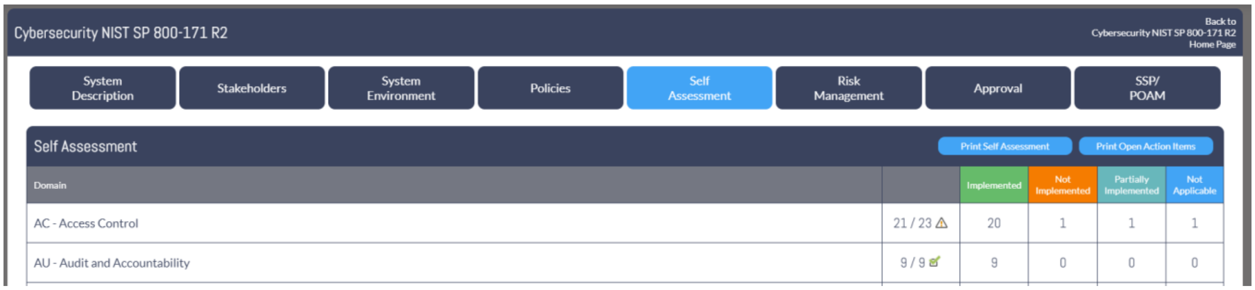


Clicking on any of the Task lists will show the Action Item Details page, where a task can be worked. Any text entered in the Response text box will be added to the audit trail for the control and files can be uploaded or linked. The files will be attached to the control, not the task. If the action is no longer needed, click on the Remove this Task checkbox and Save, you will be prompted to confirm. This will remove the action item and any associated notes, links or documents. This is only recommended if the audit of the task is not needed.

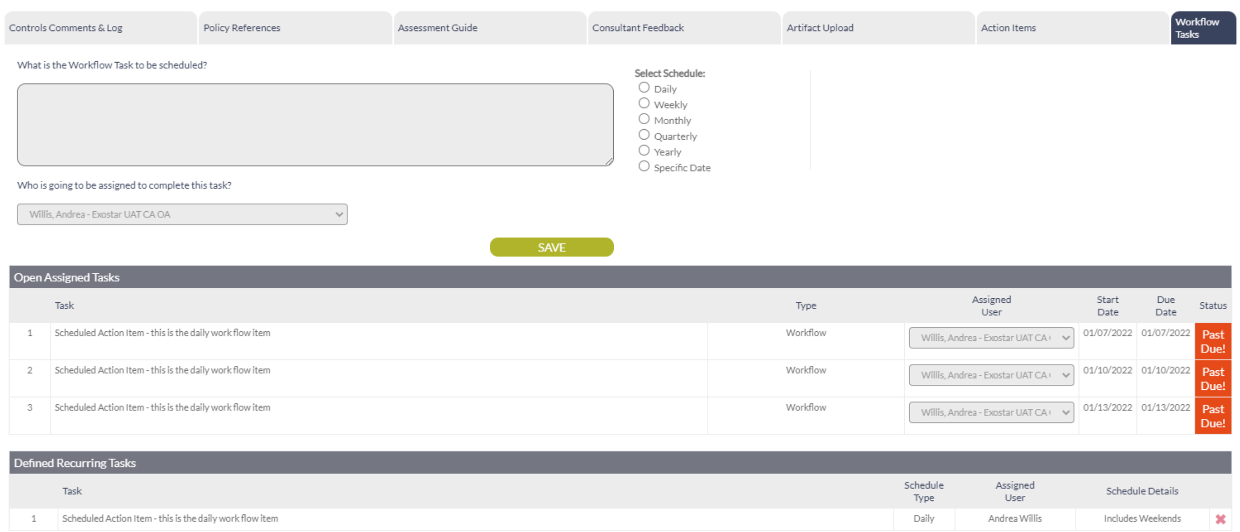
When the action is complete, click on the Close this Task checkbox and Save to close the task and return to the screen you were previously on.



You can print out all Open Action Items from the Self-Assessment Tab.

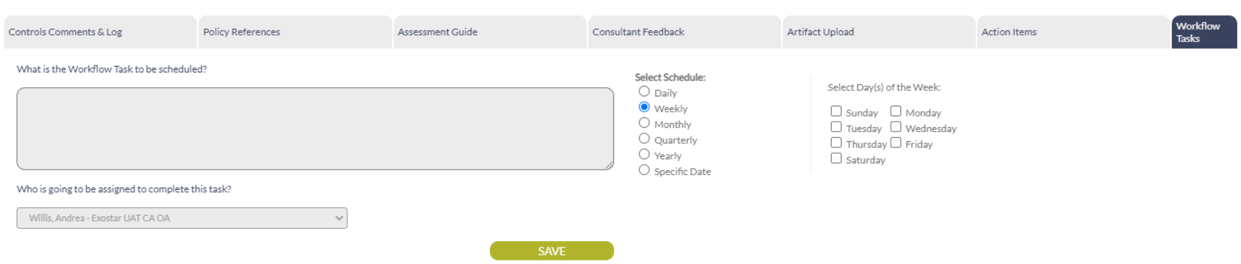


Tab 6 – Workflow Tasks



Workflow tasks are tasks that can be assigned to users on a schedule and do NOT affect the status of the control.

Schedule frequency are daily, weekly, monthly, quarterly, and yearly. There is also the ability to schedule more frequently as in twice a week, twice a month etc.

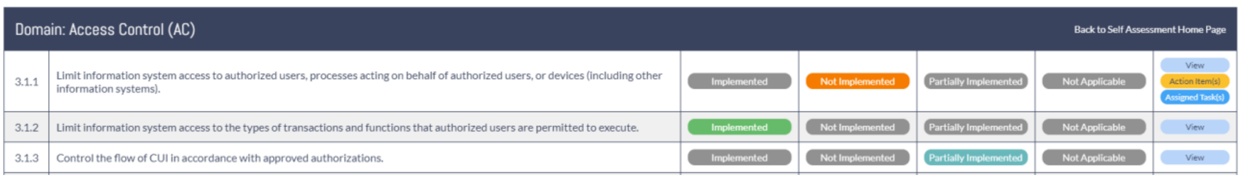


Once a task has been created you will see it in the bottom section, Defined Recurring Tasks. If no longer needed, the task can be removed by clicking the X.

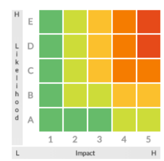
Based on the schedule of the task, the active task to be done, will be created nightly and then appear in the Open Assigned Task section. The active task will also display on the Dashboard if it is assigned to you.

Updating each active task is the same as an action item (POAMs) as shown below.

Any individual control that has a Workflow Task will now be indicate by the blue Assigned Tasks icon.



Risk Management Tab

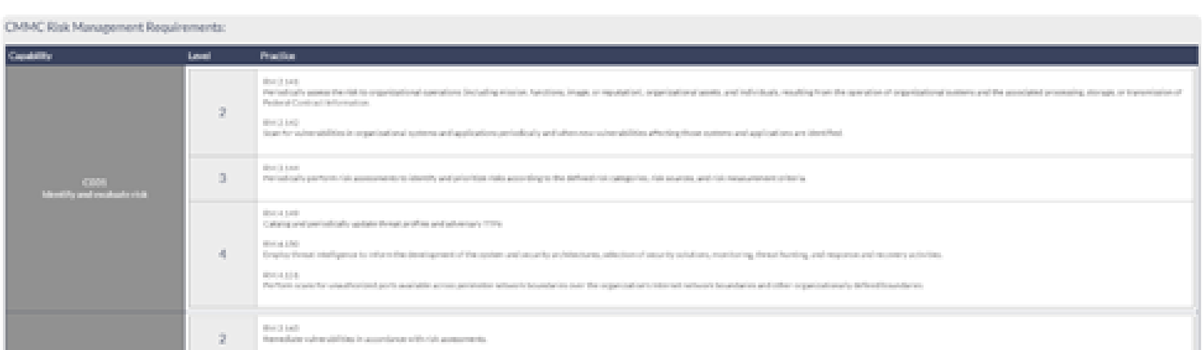


The Risk Management Tab starts with no risk identified. The blue process flow above the risk list is for user informational purposes only. These blue blocks are not linked to the specified process. Once risks are developed, they will show in the risk cube to the right.

Notes for risk cube:

- The vertical axis corresponds to the likelihood a risk will be exploited
  - A higher risk plot, corresponds to a higher likelihood the risk will be exploited
- The horizontal axis corresponds to the level of impact should the risk be exploited
  - The further to the right corresponds to a higher impact should the risk be exploited

The CMMC Risk Management Control Requirements (below) can be viewed by the user by clicking on the blue oval link just above the risk table. This matrix contains the CMMC requirements for each level of certification.

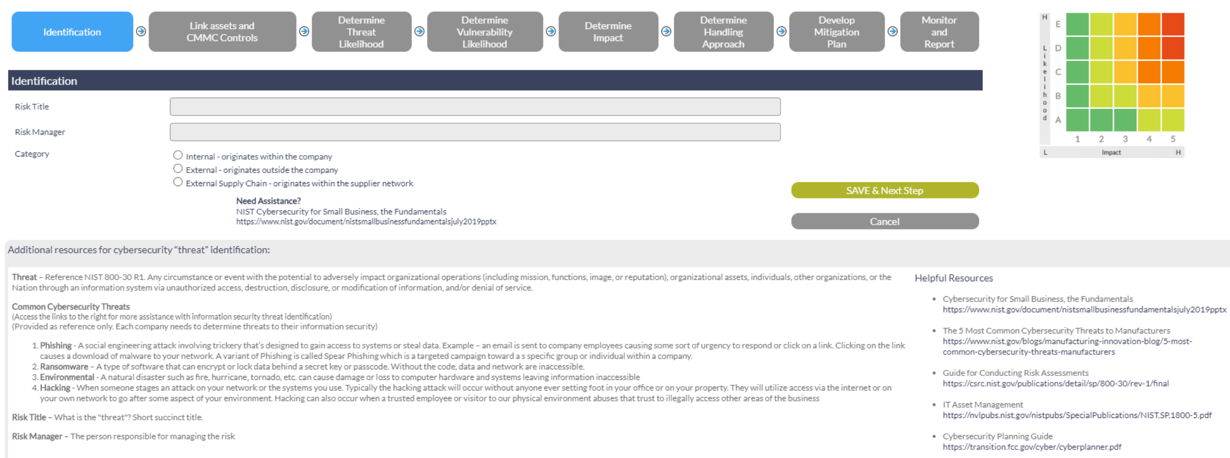


To add new risk items, the user will click on the blue “Add Risk” link

After selecting “Add Risk”, the user will see the below screen shot.

Notes for adding a new risk item:

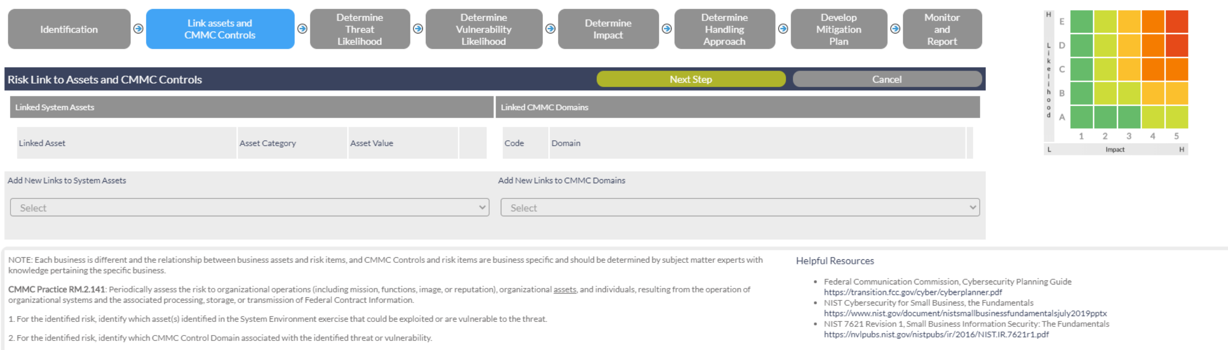
- Helpful resources are listed at the bottom of the page
- Helpful links are listed at the bottom right of the screen
  - These are external links and will open in a new tab
- The user will answer the three sections:
  - Risk Title – User should use the resource links for help
  - Risk Manager – Select from the down arrow menu
  - Category – User should select the appropriate choice



After selecting "SAVE & Next Step", the user will see the below screen shot.

Notes for linking a risk to Assets or Controls:

- Helpful resources are listed at the bottom of the page
- Helpful links are listed at the bottom right of the screen
    - These are external links and will open in a new tab
    - The user will select from the drop-down menu items (See more below)

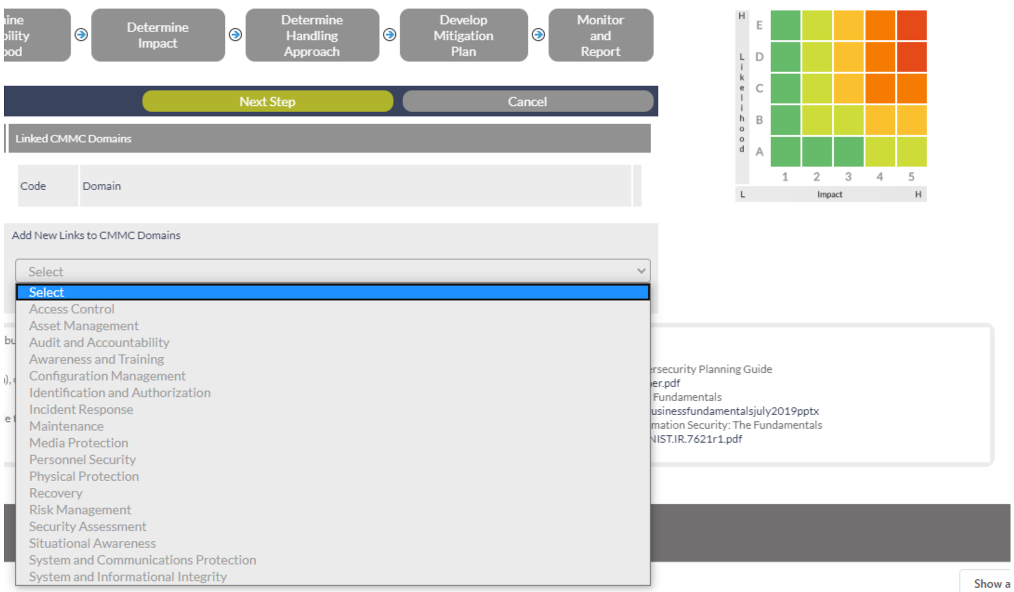


To access the list of available assets for linking to risk the user will select the drop-down menu arrow. The menu will contain a list of all assets identified during the System Environment exercise.

The user can select one or many assets. After each selection, the selected item will appear above the drop-down menu selection. An asset can be deleted if it is determined it should no longer be listed as a linked asset to the identified risk.

To access the list of available Control Domains for linking to risk, the user will select the drop-down menu arrow. The menu will contain a list of all CMMC Domains.

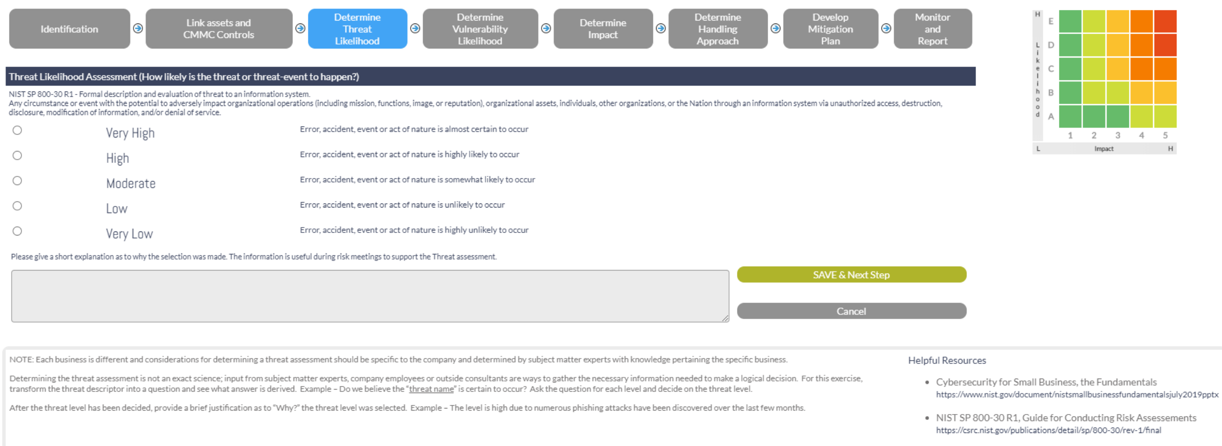
The user can select one or many Domains. After each selection, the selected item will appear above the drop-down menu selection. A Domain can be deleted if it is determined it should no longer be listed as a linked Domain to the identified risk.



After completing the risk linking to Assets and Controls, the user will select “Next Step” to move to the next screen.

Notes for Determining a Threat Assessment:

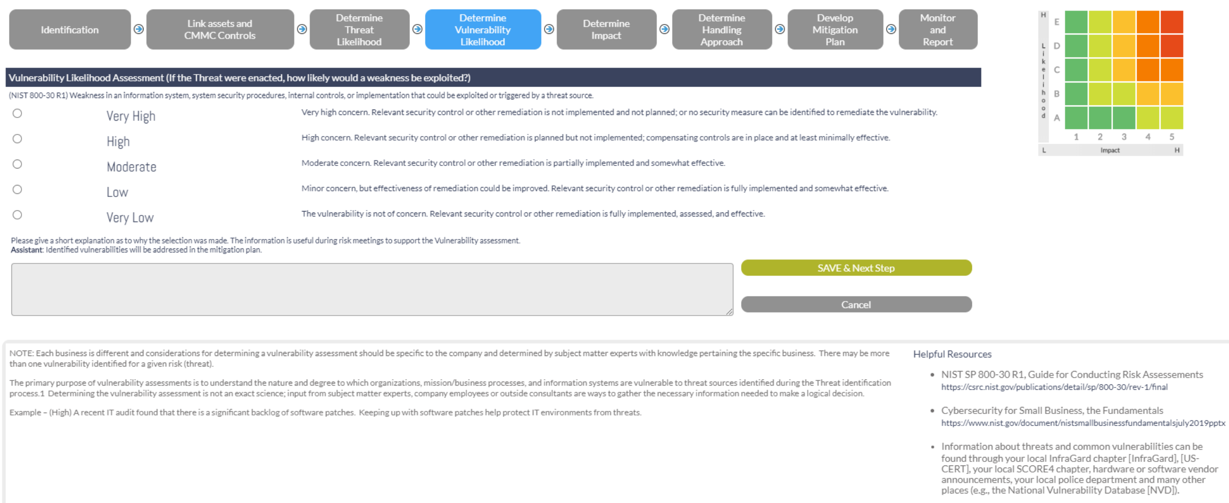
- Helpful resources are listed at the bottom of the page
- Helpful links are listed at the bottom right of the screen
    - These are external links and will open in a new tab
- The user will select the Threat level by clicking the radio button that corresponds to the appropriate description
- After selecting a threat level, the user should provide a short narrative as the "why" the threat level was selected. While this is not a requirement, it is highly recommended.



Once complete, the user will select "SAVE & Next Step" to move to the next screen.

Notes for Determining a Vulnerability Assessment:

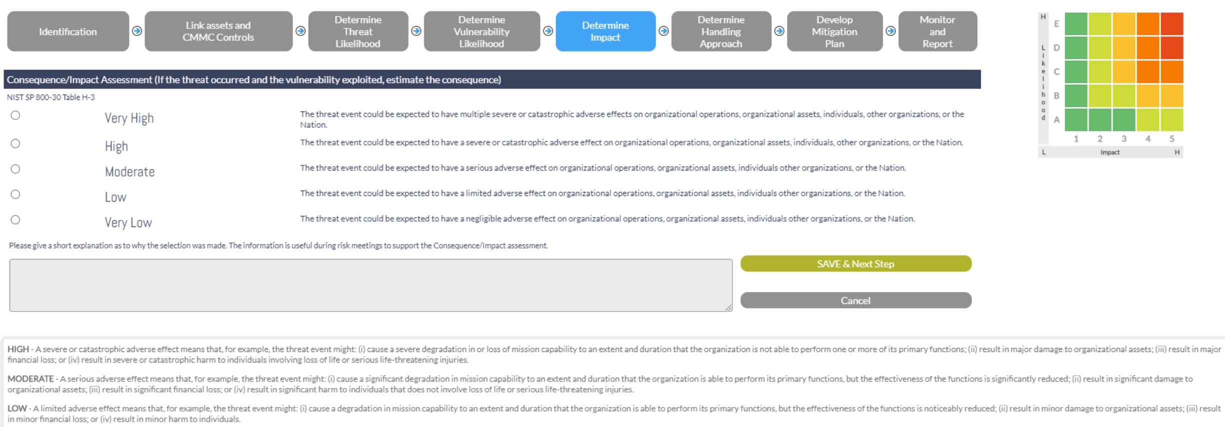
- Helpful resources are listed at the bottom of the page
- Helpful links are listed at the bottom right of the screen
  - These are external links and will open in a new tab
- The user will select the vulnerability level by clicking the radio button that corresponds to the appropriate description
- After selecting a vulnerability level, the user should provide a short narrative as the "why" the level was selected. While this is not a requirement, it is highly recommended.



Once complete, the user will select “SAVE & Next Step” to move to the next screen.

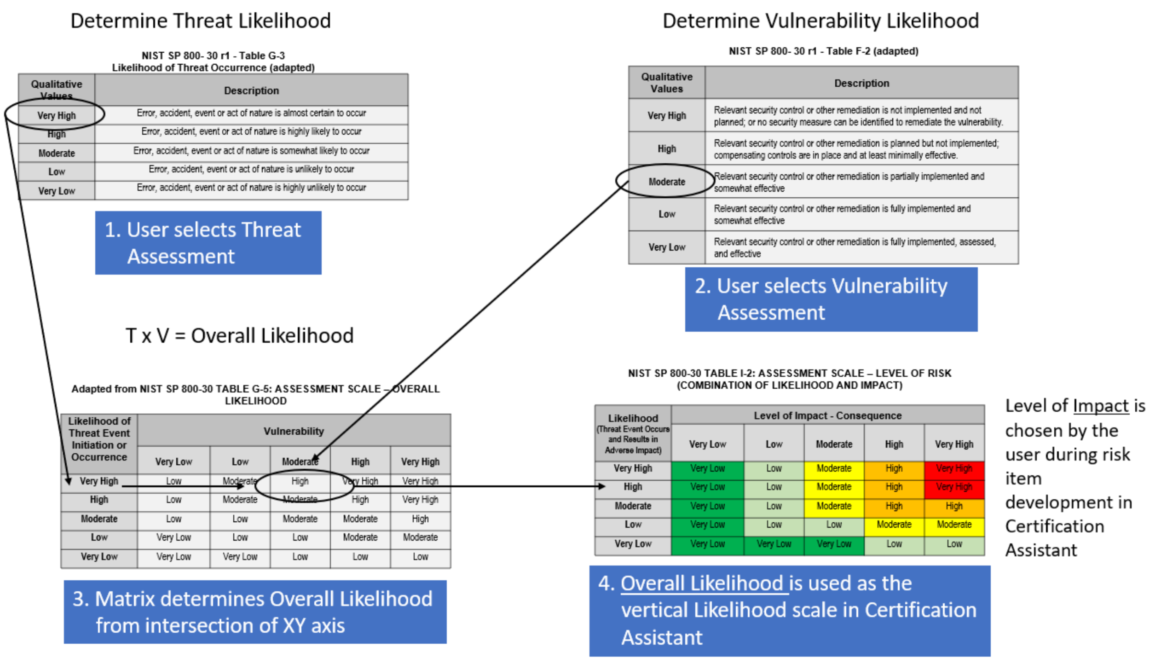
Notes for Determining an Impact Assessment:

- Helpful resources are listed at the bottom of the page
- Helpful links are listed at the bottom right of the screen
    - These are external links and will open in a new tab
- The user will select the impact level by clicking the radio button that corresponds to the appropriate description
- After selecting an impact level, the user should provide a short narrative as the “why” the level was selected. While this is not a requirement, it is highly recommended.



Once complete, the user will select “SAVE & Next Step” to move to the next screen.

Guide for discussing the Overall Risk Likelihood Calculation



Notes for Determining a Handling Approach:

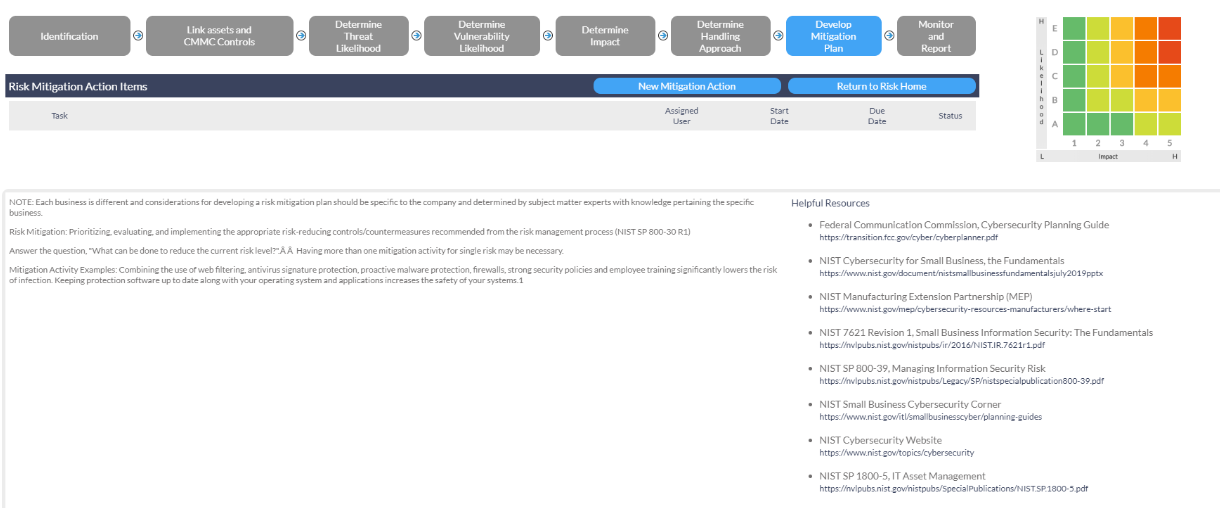
- User will have one of three choices:
  - Accept the Risk – Instructions are provided on-screen
  - Transfer the Risk – Instructions are provided on-screen
  - Mitigate the Risk – Instructions are provided on-screen
- Once the Handling Approach is selected, the user will populate the Risk Handling Approach Justification and Plan. This field will be useful during risk meetings when discussing risk strategy with company leaders and subject matter experts
- User selects “SAVE and Next Step”
- **NOTE:** Only when choosing Mitigate the Risk does the user proceed to the next step, which is developing a mitigation plan. SEE NEXT SCREEN SHOT

Notes for creating a mitigation step:

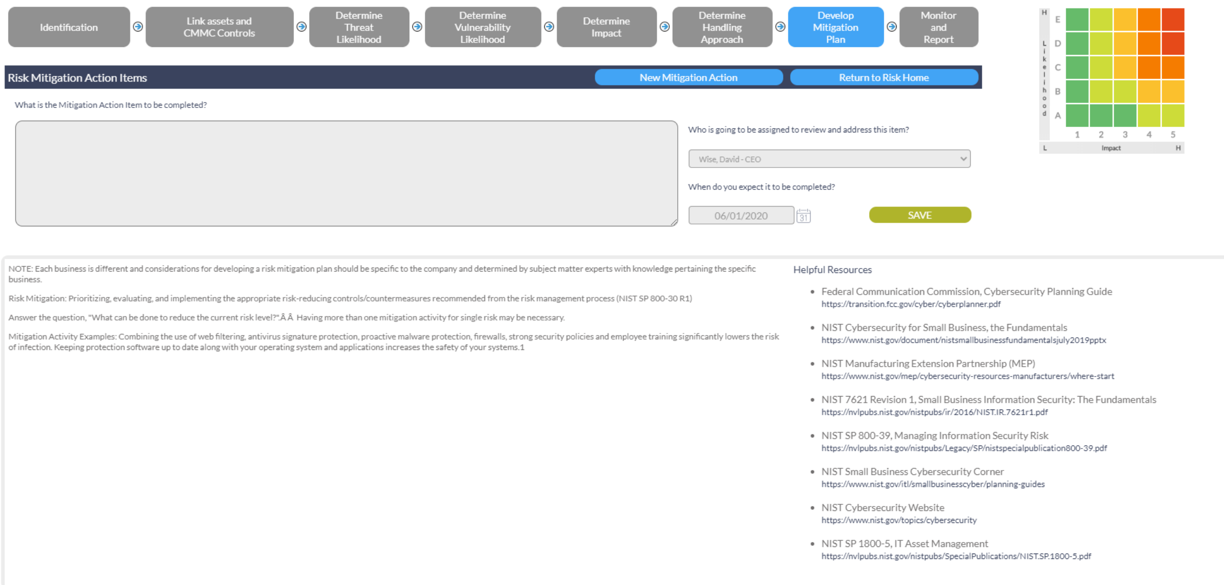
- User will click on New Mitigation Action 

  - The second screen shot below will appear
  - User will describe what mitigation activity will be performed by filling in the text window
  - User will select the person responsible for the activity
  - User will assign a completion date for the activity

- User selects "SAVE"
- User has an option to create another mitigation activity or Return to Risk Homepage.



EXOSTAR®



Notes for Monitor and Report:

- There are no specific notes for this. 

    - User will see all mitigation actions on the TASKS list located on the Certification Standard Homepage
    - User will see status of all mitigation actions on the TASKS list located on the Certification Standard Homepage

- The below guide comes directly from NIST SP 800-30 r1. Since there are not specific tool functions for Monitor and Report, this guide gives the user some ideas on what should be done during the activity of risk management. It will also help during certification if the company can demonstrate monitoring and reporting activity.

Key Activities for risk monitoring and reporting (NIST 800-30 r1)

Monitoring - Summary of Key Activities

Maintaining Risk Assessments

i. Identify key risk factors that have been identified for ongoing monitoring.
ii. Identify the frequency of risk factor monitoring activities and the circumstances under which the risk assessment needs to be updated.
iii. Reconfirm the purpose, scope, and assumptions of the risk assessment.
iv. Conduct the appropriate risk assessment tasks, as needed.
v. Communicate the subsequent risk assessment results to specified organizational personnel.

Reporting – Summary of Key Activities

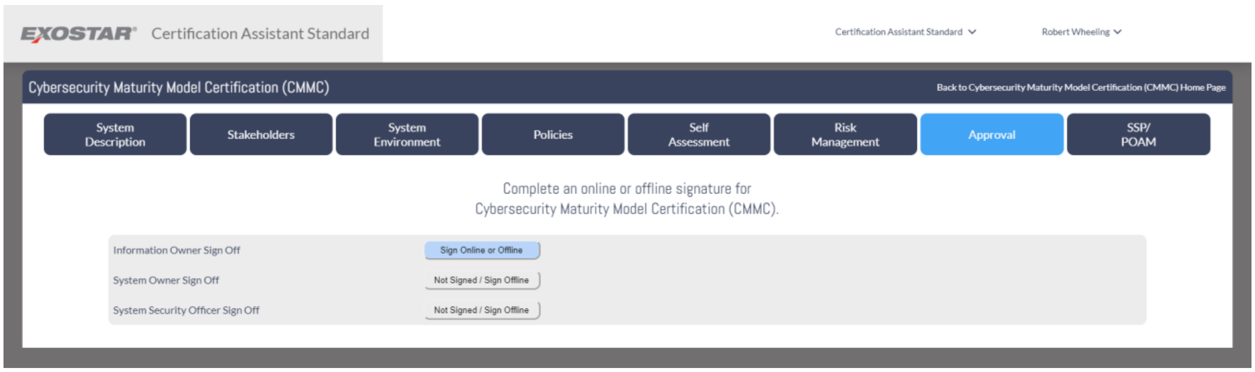
(Also known as Communication and Sharing)

Maintaining Risk Assessments

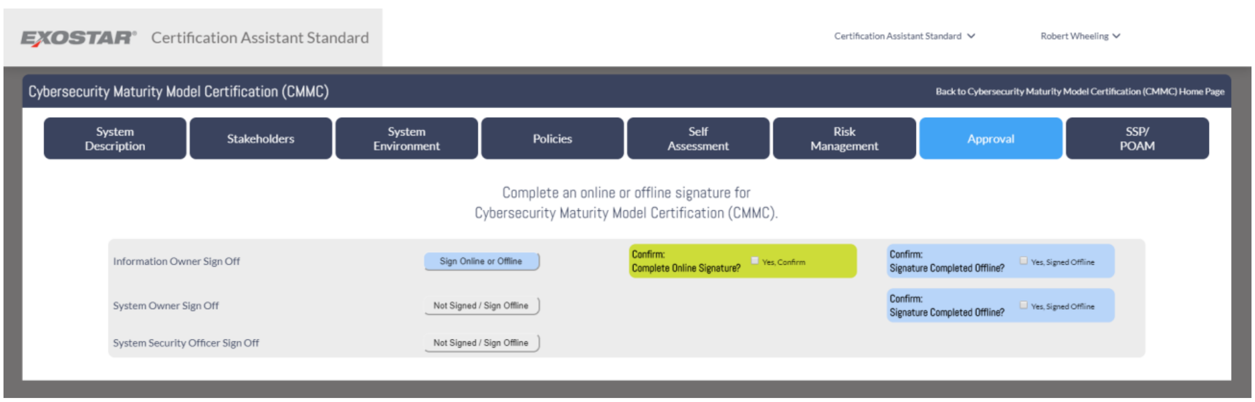
i. Determine the appropriate method (e.g., executive briefing, risk assessment report, or dashboard) to communicate risk assessment results.
ii. Communicate risk assessment results to designated organizational stakeholders.
iii. Share the risk assessment results and supporting evidence in accordance with organizational policies and guidance.

Approval Tab

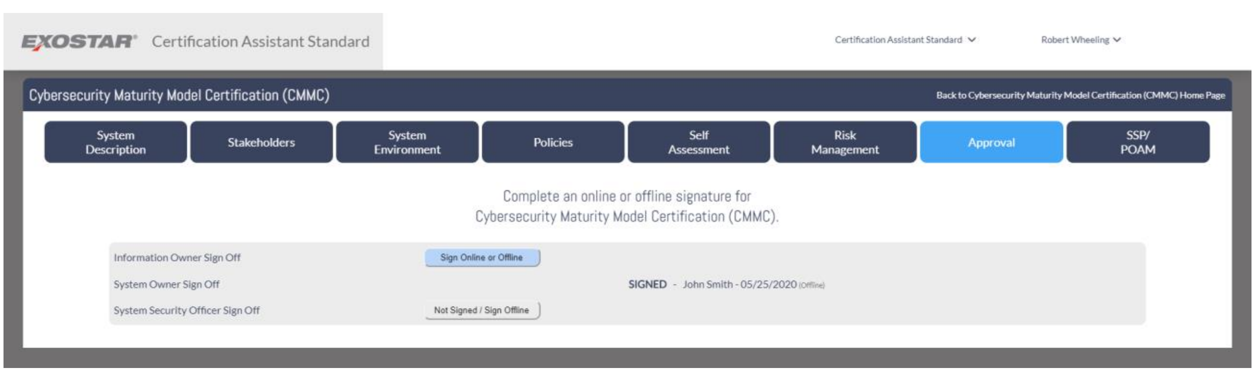
After all the content has been added to the tabs, the Approval tab can be used to sign the content either online or offline. Online signatures can be accomplished by the user if their name was linked to the information on the Stakeholders tab. If online signature is available, the blue Sign Online or Offline button is available. If Offline is the only option, then the grey Not Signed/Sign Offline button is available.



Click on the buttons to enable signing, and then click on the checkbox for the option to be used. Note: only one signature at a time will be processed.



When the signature is complete, the name, date and method will be shown.

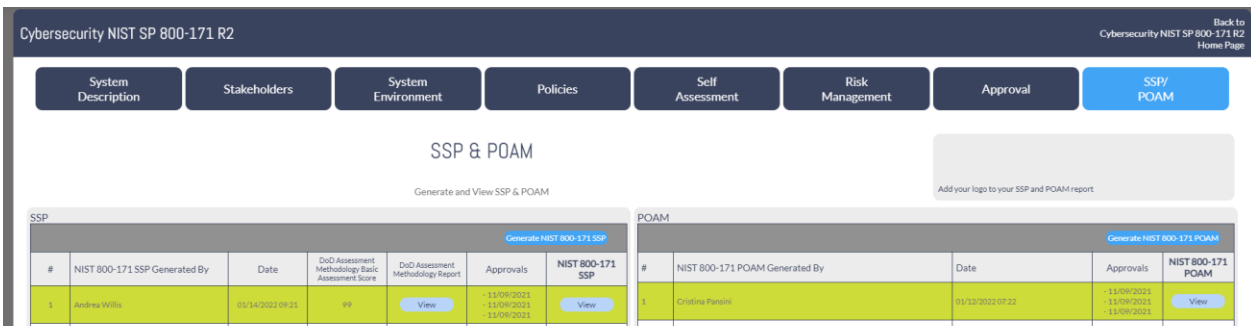


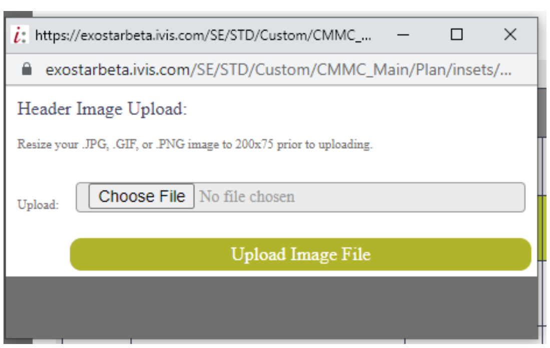
SSP/POAM Tab

The final tab is the SSP/POAM tab for reporting the System Security Plan and Plan of Action and Milestones (POAM). Each of the reports are the moment in time the generate button is selected and cannot be revised when it is generated. To create an SSP report, click on the Generate SSP button or the Generate POAM button to create a POAM.

You now have the ability to add your own logo to both the SSP and POAM reports.

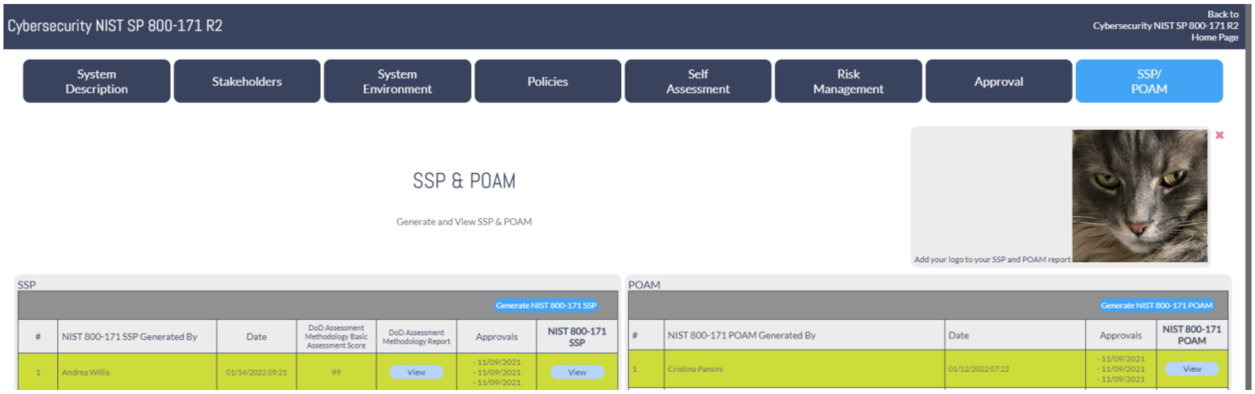
Note: Logo must be jpg, gif or png format in a size of 200 by 75 to fit.

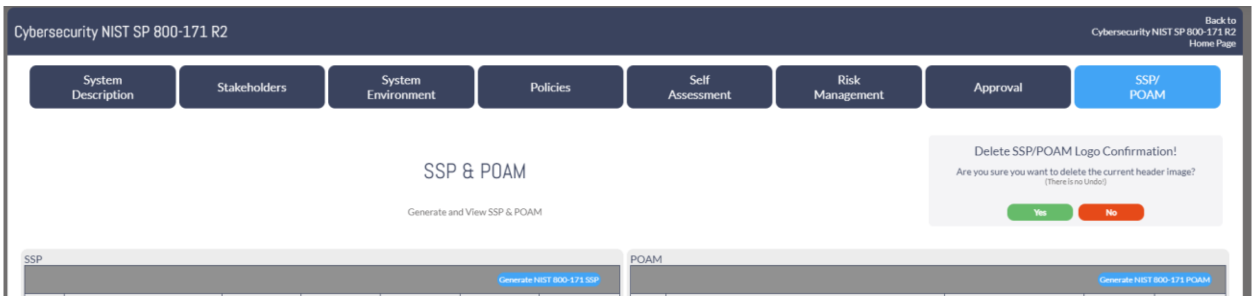




If you put the wrong log as shown with the cat – just select the x to the right and the system will prompt to confirm removal.

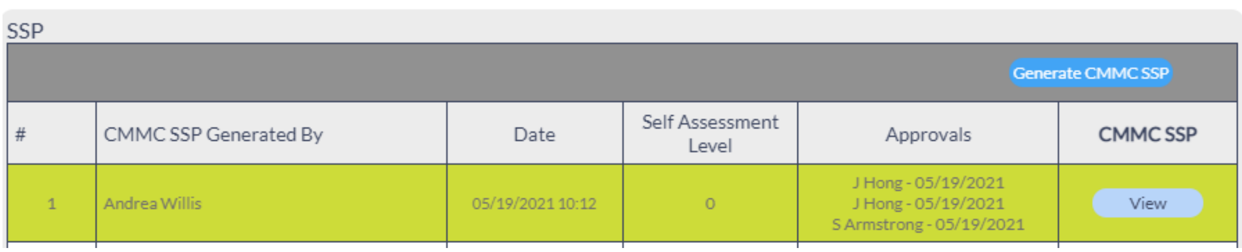
Any SSP or POAM generated with a deleted image will show a blank spot. Any newly generated SSP or POAM will then show the default Exostar logo.





SSP and POAM reports can be created for either CMMC or on NIST 800-171. The most recent document will be highlighted in green.

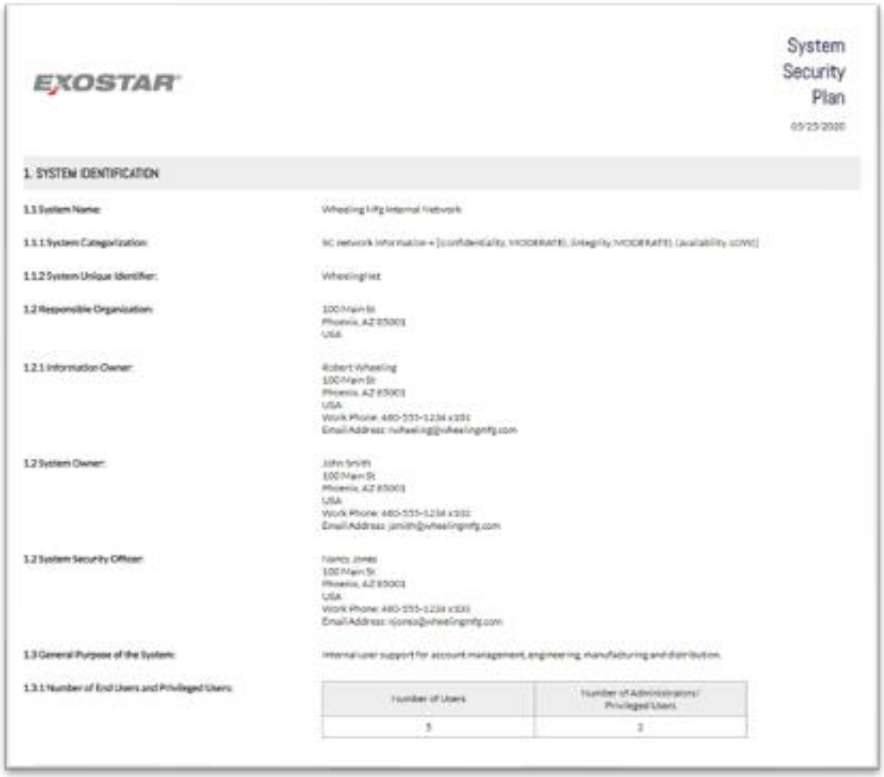
To view the generated report, click on the View button.


SSP

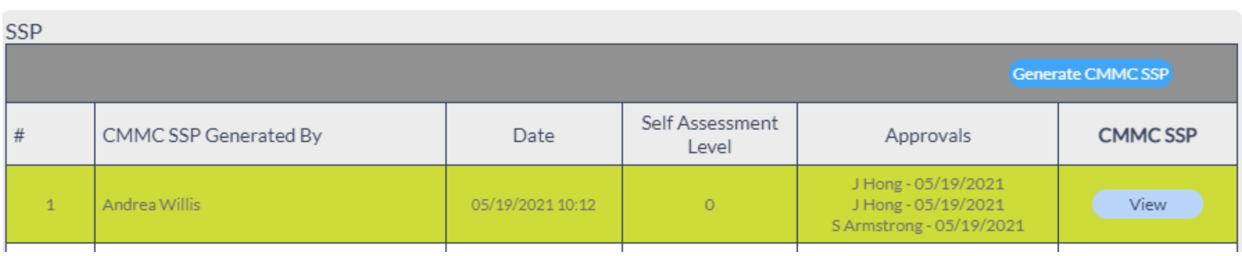
Generate CMMC SSP

#	CMMC SSP Generated By	Date	Self Assessment Level	Approvals	CMMC SSP
1	Andrea Willis	05/19/2021 10:12	0	J Hong - 05/19/2021 J Hong - 05/19/2021 S Armstrong - 05/19/2021	View

The screenshot below is an example of the SSP report.



In addition to the SSP, the DoD Basic Assessment Report is generated. Click on the View button to see the report. You can use this to submit to DOD SPRS. Note: DoD Basic Assessment report is only available in NIST 800-171.



SSP

#	NIST 800-171 SSP Generated By	Date	DoD Assessment Methodology Basic Assessment Score	DoD Assessment Methodology Report	Approvals	NIST 800-171 SSP
1	Scott Armstrong	06/08/2021 12:42	N/A	View	J Hong - 06/08/2021 J Hong - 06/08/2021 S Armstrong - 06/08/2021	View
2	Scott Armstrong	05/26/2021 14:13	58	View	J Hong - Not Signed J Hong - Not Signed S Armstrong - Not Signed	View

Generate NIST 800-171 SSP

Click on the View button to preview the POAM report.

POAM

Generate NIST 800-171 POAM

#	NIST 800-171 POAM Generated By	Date	Approvals	NIST 800-171 POAM
1	Jungbo Hong	08/04/2020 08:20	-	View

Plan of Action & Milestones

05/25/2020

	Plan	Task	Assigned User	Start Date	Due Date	Status
1	Cybersecurity Maturity Model Certification (CMMC) / 2020	Action Item - Update and post Privacy notices	Robert Wheeling	05/25/2020	05/30/2020	New
		• 05/25/20 04:07:34 PM PDT by Robert Wheeling - STATUS CHANGED via PIM Import: Not Implemented				

Certification Assistant Messaging

Message notifications are found in the upper right next to your username.

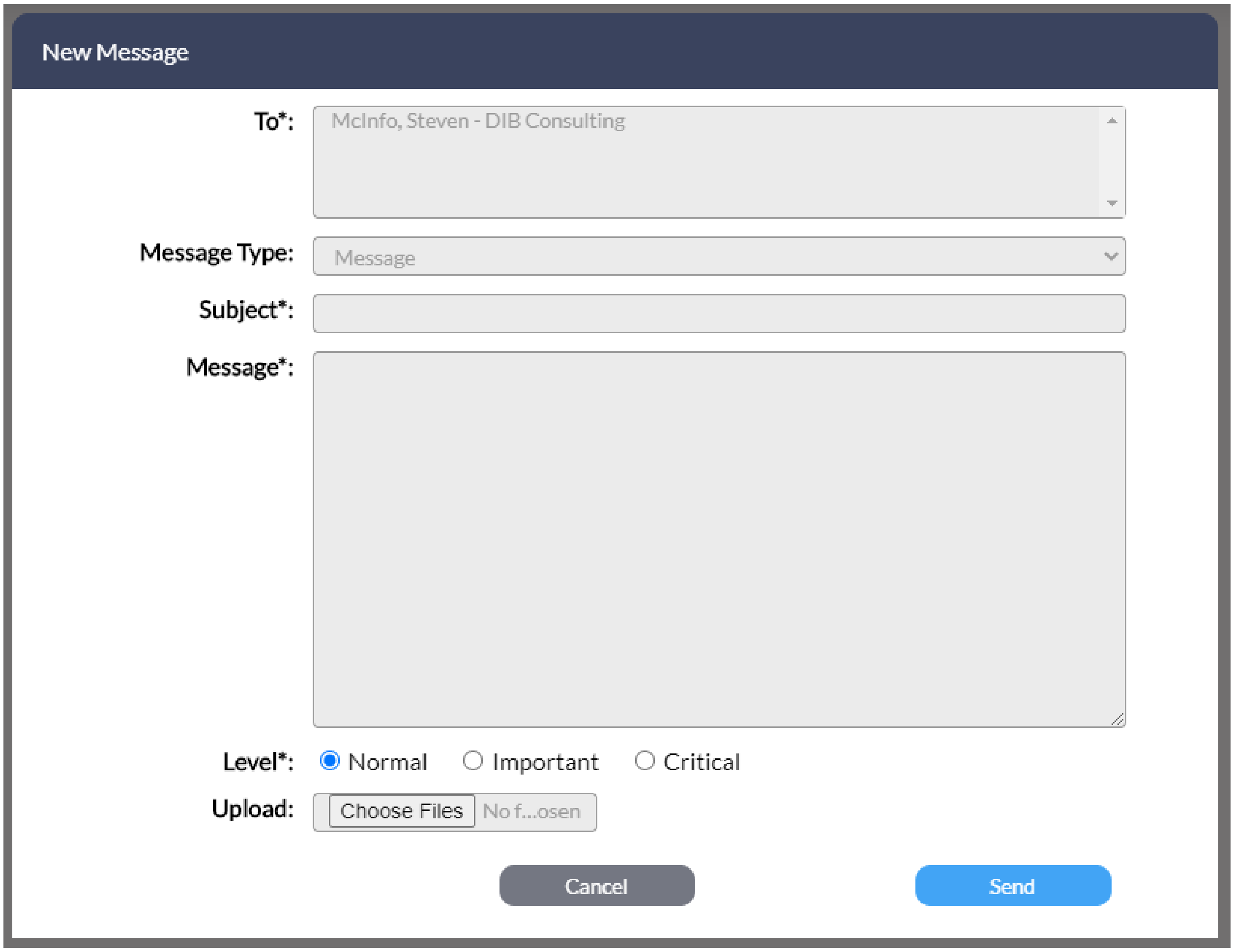
David Wise 0

If the number next to the bell is higher than 0, then you have new messages waiting.

Your messages will appear in the Message Inbox on the homepage.

To increase the size of the window, click on the Message Inbox button and the messages feature will go to full screen.

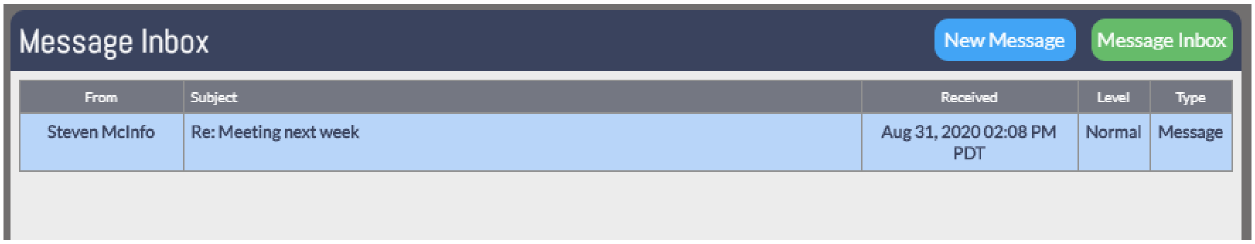
To send a message, click on the New Message button.



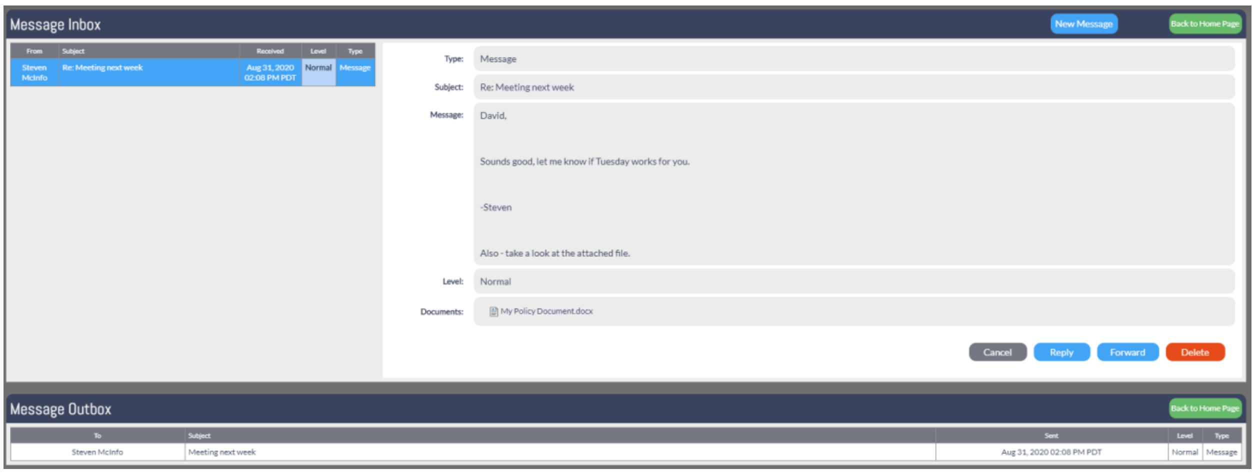
The required fields are flagged with an asterisk (*). Select one or multiple users from the To box. Use the CTRL or Apple key to select multiple. All users within your account and any consultants you are currently engaged with will be available on the list. To see more about consultants, see the Partner Engagement section.

Select your Message Type, enter a subject and enter your message. Select the Level for the message and attach files if needed. Any files attached will be uploaded and encrypted. Click the Send button and the message will show up in your sent list.

New messages will be highlighted blue and always at the top of the list.



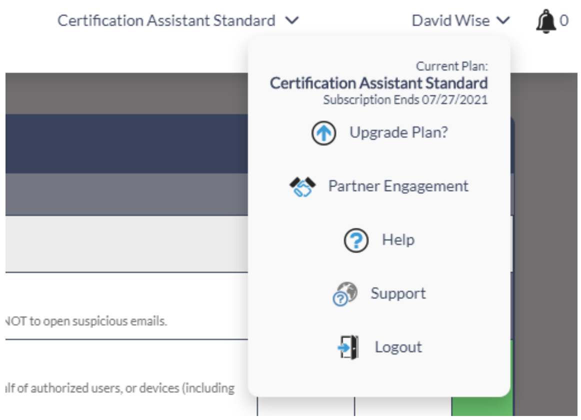
Click on the message to view.



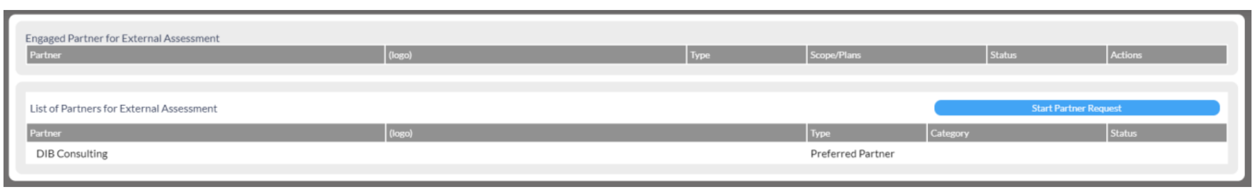
To reply to this message, click on the Reply button and Send when your message is complete. Similarly, to Forward to another user, click on Forward and Send when your message is complete.

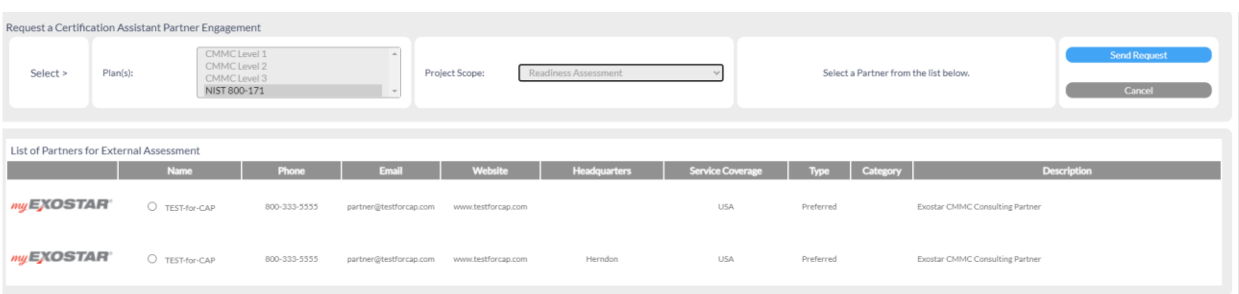
Partner Engagement

The Partner Engagement feature enables Certification Assistant users to engage consultant partners of Exostar to perform assessments on the practices and processes of CMMC prior to seeking certification. To start an engagement, click on the down arrow next to your name in the upper right portion of the page and select Partner Engagement.

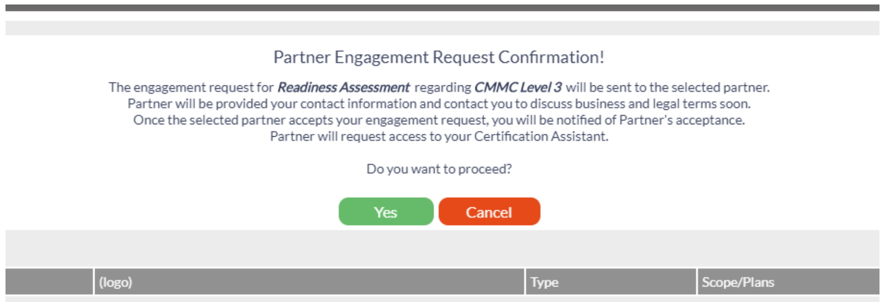


To begin, click on the Start Partner Request button.





Select the Plan(s) to be assessed, CMMC Level 1, 2 or 3 or NIST 800-171. Project Scope is locked to Readiness Assessment (more options coming later) and then select the partner you intend to work with from the list provided. Click the Send Request button and you will be prompted with:

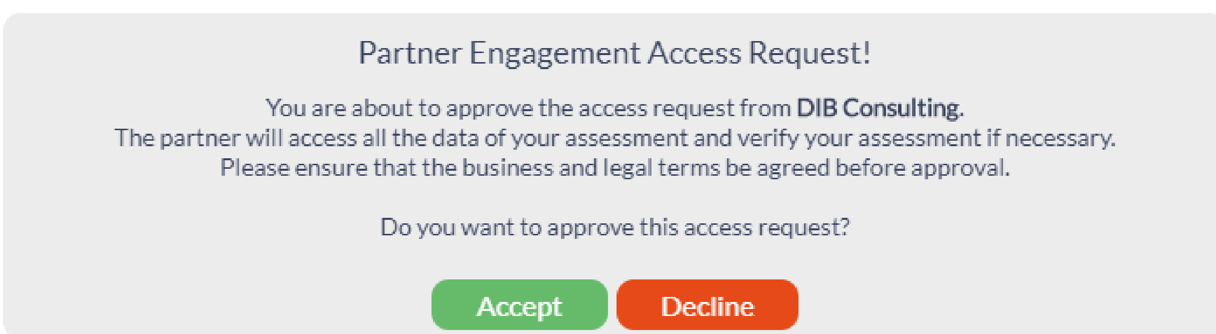


Click on Yes to confirm that you want to proceed, although you have the option to terminate the engagement at any time.

The partner will be notified through the messaging system and will be prompted to Accept or Reject the engagement. All contract terms and conditions for the Partner engagement occur outside of Certification Assistant. Once a decision has been made, then return to Certification Assistant to status the relationship.

Once accepted, the status will update to Engagement Accepted. The partner will then assign a consultant to your engagement and they will request access to your data in Certification Assistant. You will receive a message from the system that this request has been sent.

Return to the Partner Engagement function and you have the option to Accept or Decline access to your data.



If you choose to accept, the consultant will be able to access your data from their login and review, make comments, assign actions, and upload documentation just like a member of your account. When they have completed their work, they will cancel access and move on to the documentation stage of the project.

EXOSTAR®

At any time you have the ability to terminate the relationship and access to Certification Assistant, click the Terminate Engagement.

Type	Scope/Plans	Status	Actions
Preferred Partner	Readiness Assessment / CMMC Level 3 From: 08/31/2020	Assessment Complete Access Disconnected	Terminate Engagement

When the consultant has completed the documentation report, they will deliver it to you via the system and you will receive another message. In the Partner Engagement screen, click on the View Documentation to review the report.

Type	Scope/Plans	Status	Actions
Preferred Partner	Readiness Assessment / CMMC Level 3 From: 08/31/2020	Assessment Delivered	Terminate Engagement View Documentation

The project can then be closed by the consultant and the overall engagement can be terminated by you or the consultant partner administration. You will still have access to the documentation and at any time you can click on the New Engagement button to start another project.

Scope/Plans	Status	Actions
Readiness Assessment / CMMC Level 3 From: 08/31/2020 To: 08/31/2020	Engagement Completed	View Documentation
	New Engagement	

Partners and their customers can now share documents during the engagement. These are any documents … not the Assessment at the end of an engagement. Note that when an engagement ends access to any shared documents is also removed.

Scope/Plans	Status	Actions
Readiness Assessment / CMMC Level 3 From: 10/08/2021 To: 12/07/2021	Engagement Completed	
Readiness Assessment / CMMC Level 1 From: 10/29/2021	Request Engagement	Cancel Request Document Share