



Certification Assistant Standard & Premium User Guide January 2022

The Exostar logo, consisting of the word 'EXOSTAR' in a bold, sans-serif font with a red and white stylized 'X' to its left. The logo is centered and overlaid on a background of several intersecting red and grey lines that form a large, abstract geometric shape.

EXOSTAR[®]

CONTENTS

Document Versions.....	3
Certification Assistant Standard & Premium Help.....	5
Certification Assistant Standard & Premium Home Page	5
Import / Export.....	6
Cybersecurity Maturity Model Certification (CMMC) Home Page	7
System Description Tab	10
Stakeholders Tab.....	12
System Environment Tab	13
Policies Tab	15
Self-Assessment Tab.....	16
Tab 1 – Controls Comments & Log	19
Tab 2 – Policy Reference.....	19
Tab 3 – Assessment Guide	20
Tab 4 – Artifact Upload.....	20
Tab 5 – Action Items.....	21
Risk Management Tab	24
Approval Tab	35
SSP/POAM Tab.....	36
Certification Assistant Messaging.....	39
Partner Engagement.....	43

DOCUMENT VERSIONS

Version	Impacts	Date
Certification Assistant		Pre-June 2021
CA 1.4	<p>1.4 includes:</p> <ul style="list-style-type: none"> • Dashboard redesign • Export • Printing Updates • Update to Individual Self-Assessment: <ul style="list-style-type: none"> ○ New Tab structure <ul style="list-style-type: none"> ▪ 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	<p>1.5 includes:</p> <ul style="list-style-type: none"> • 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	<p>1.6 includes:</p> <ul style="list-style-type: none"> • Ability to upload software and hardware system configurations using standard templates. • Ability to change an Action Item type after it's been created <ul style="list-style-type: none"> ▪ From NIST to CMMC or BOTH 	

	<ul style="list-style-type: none">▪ 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<ul style="list-style-type: none">▪ These do NOT change the status of the control▪ These do show up on the dashboard and the individual control page• Improved Navigation<ul style="list-style-type: none">▪ 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	
--	---	--

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.

The screenshot displays the Certification Assistant Home Page with the following sections:

- Plans:** Two buttons for "Cybersecurity Maturity Model Certification (CMMC)" and "Cybersecurity NIST SP 800-171 R2". Below are progress charts for CMMC (12%, 44%, 40%, 100%, 100%) and NIST SP 800-171 (97%). A "DvD Assessment Score for SPRS" of 99 is shown with an estimated completion date of 01/06/2022.
- Organization Activity Highlights:**
 - CMMC:** Overdue POAMs: 1, POAMs Due within 90 Days: 0, % with Implementation Statements: 3%, % with Evidence and/or Policies: 0%
 - NIST SP 800-171:** Overdue POAMs: 1, POAMs Due within 90 Days: 0, % with Implementation Statements: 4%, % with Evidence and/or Policies: 0%
 - Risk Management:** Risk Register Items Initiated: 4, Risk Register Items Fully-Managed: 2
- Tasks:** A table listing 5 tasks, all marked as "Past Due!".

Task	Type	Start Date	Due Date	Status
1. CMMC - Level 1 - AC 1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Action Item - This is the follow up text.	NIST POAM	01/06/2022	01/06/2022	Past Due!
2. CMMC - Level 1 - AC 1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Scheduled Action Item - This is the daily work flow item	ActionItem/Workflow	01/07/2022	01/07/2022	Past Due!
3. CMMC - Level 1 - AC 1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Scheduled Action Item - This is the daily work flow item	ActionItem/Workflow	01/10/2022	01/10/2022	Past Due!
4. CMMC - Level 3 - AC.3.019 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Terminate (automatically) user sessions after a defined condition. Scheduled Action Item - This is a test of a workflow task	ActionItem/Workflow	01/13/2022	01/13/2022	Past Due!
5. CMMC - Level 1 - AC 1.001 Cybersecurity - NIST SP 800-171 R2 - 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Scheduled Action Item - This is the daily work flow item	ActionItem/Workflow	01/13/2022	01/13/2022	Past Due!
- Message Inbox:** A table showing 4 messages.

From	Subject	Received	Level	Type
No Reply	PIM Import Information	Nov 23, 2021 09:46 AM PST	Normal	Message
Andrea Willis	Access Request Notification	Oct 6, 2021 12:01 PM PDT	Important	Message
Duncan Wilson	Access Request Notification	Oct 7, 2021 09:23 AM PDT	Important	Message
Scott Armstrong	Access Request Notification	Aug 24, 2021 12:28 PM PDT	Important	Message
- Help & Profile:** Buttons for Help, Support, Import / Export, and UPGRADE!

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.

Import / Export Certification Assistant Data

Import to Certification Assistant

Select Import Option:

Upload the file here: No file chosen

Overwrite existing information:
If chosen, the import process will overwrite previously entered information in the System Description, System Environment, and control/practice Status and Implementation Statements. Implementation Statements that are overwritten will be added to the audit trail for the selected task.

Do NOT Overwrite Existing Information:
If chosen, the import process will only import information if existing System Description, System Environment and control/practice Implementation Statements are not present.

Overwrite Existing Information
 Do NOT Overwrite Existing Information

Export from Certification Assistant

Select Export Option:

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 screenshot displays the Exostar Certification Assistant Standard interface for Cybersecurity Maturity Model Certification (CMMC). At the top, there is a navigation bar with the Exostar logo, the text "Certification Assistant Standard", and a green button labeled "UPGRADE to Certification Assistant Premium Click Here!". On the right side of the navigation bar, there are dropdown menus for "Certification Assistant Standard" and "David Wise", along with a notification bell icon.

Below the navigation bar, the main content area is titled "Cybersecurity Maturity Model Certification (CMMC)" and includes a "Back to Home Page" link. A tab toolbar at the top of the main content area contains buttons for "System Description", "Stakeholders", "System Environment", "Policies", "Self Assessment", "Risk Management", "Approval", and "SSP/POAM".

The main content area features a "Summary" section with a "Switch to NIST 800-171 View" button. Below this, a table shows the current and target CMMC levels, self-assessed CMMC level, and counts for implemented, partially implemented, not implemented, and not applicable items.

Current CMMC Level	Target CMMC Level	Self Assessed CMMC Level	Implemented	Partially Implemented	Not Implemented	Not Applicable
0	3	1	110	0	0	0

Below the summary, a "Progress Toward Certification" table provides a detailed view of progress across various domains and levels. The table includes columns for 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, and Progress to Target Level 3.

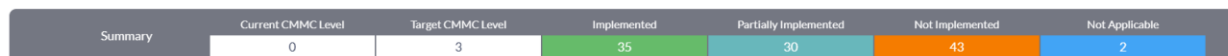
Domain	Practice/Process	Level 1 Complete/Total	Level 2 Complete/Total	Level 3 Complete/Total	Level 4 Complete/Total	Level 5 Complete/Total	Self Assessment Level	Progress to Target Level 3
Access Control	Practices	Completed 4/4	Completed 10/10	Completed 8/8			Level 3	100%
	Processes		Incomplete 0/2	Incomplete 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 2/4	In Progress 6/7			Level --	82%
	Processes		Incomplete 0/2	Incomplete 0/1			Level --	0%
Awareness and Training	Practices		Completed 2/2	Completed 1/1			Level 3	100%
	Processes		Incomplete 0/2	Incomplete 0/1			Level --	0%
Configuration Management	Practices		Completed 6/6	Completed 3/3			Level 3	100%
	Processes		Incomplete 0/2	Incomplete 0/1			Level --	0%
	Procedures	Completed	Completed	Completed			Level 3	100%

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.



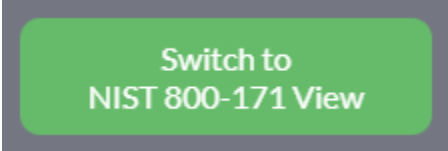
The Progress Toward Certification table gives a complete progress in each CMMC domain toward your goal certification level.

Progress Toward Certification								
Domain	Practices/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 3/10	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%

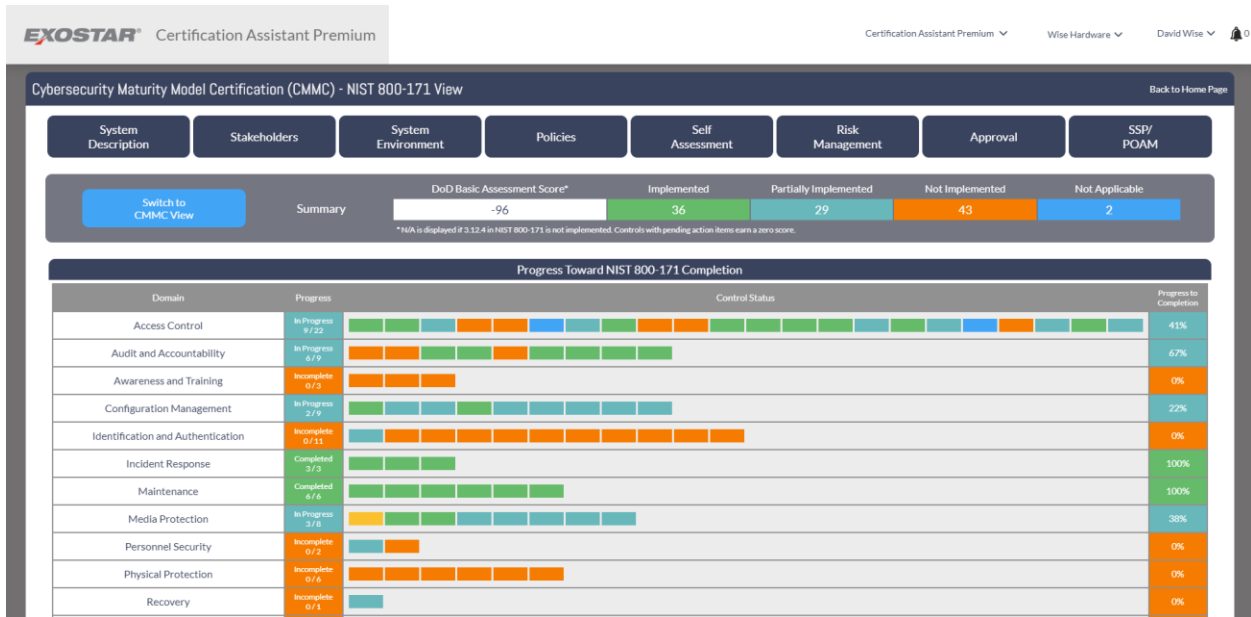
How to read the chart:

- 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.

Progress Toward NIST 800-171 Completion			
Domain	Progress	Control Status	Progress to Completion
Access Control	In Progress 22 / 23		96%
Awareness and Training	Completed 3 / 3		100%
Audit and Accountability	Completed 9 / 9		100%
Security Assessment	Completed 4 / 4		100%
Configuration Management	Completed 9 / 9		100%
Identification and Authentication	Completed 11 / 11		100%
Incident Response	Completed 3 / 3		100%
Maintenance	Completed 6 / 6		100%
Media Protection	Completed 9 / 9		100%
Physical Protection	Completed 6 / 6		100%
Personnel Security	Completed 2 / 2		100%
...	Completed		100%

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.

Cybersecurity Maturity Model Certification (CMMC) Back to Cybersecurity Maturity Model Certification (CMMC) Home Page

System Description

Stakeholders

System Environment

Policies

Self Assessment

Risk Management

Approval

SSP/POAM

Edit

System Name/Title	CUI Management System
State the name of the system. Spell out acronyms.	
System Scope	--
System Categorization	Moderate Internal system
System CAGE Code(s)	3ABC1
System Unique Identifier	SYS0001
Insert the System Unique Identifier	
Responsible Organization	Name: Exostar
	Address: Exostar Way Herndon, VA 22209 America
	Phone: 888-888-1234
General Purpose of the System	Secure Contractor Systems for securely managing CUI.
Provide a short, high-level description of the function/purpose of the system.	
Number of end users and privileged users	End Users: 25 Privileged Users: 1
In the fields above, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc.	
General description of information	CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list . <small>(Document the CUI information types processed, stored, or transmitted by the system below.)</small>

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.

EXOSTAR® Certification Assistant Standard Certification Assistant Standard ▾ Robert Wheeling ▾

Cybersecurity Maturity Model Certification (CMMC) Back to Cybersecurity Maturity Model Certification (CMMC) Home Page

System Description | Stakeholders | System Environment | Policies | Self Assessment | Risk Management | Approval | SSP/POAM

Save Cancel

System Name/Title: Wheeling Mfg Internal Network
State the name of the system. Spell out acronyms.

System Categorization: SC network information = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}

System Unique Identifier: WheelingMfg1234
Insert the System Unique Identifier

Responsible Organization: Name: Robert Wheeling
Address: Street: 100 Main St
City: Phoenix State: AZ Zip: 85001 Country: USA
Phone: 480-555-1234

General Purpose of the System: Internal user support for account management, engineering, manufacturing and distribution.
Provide a short, high-level description of the function/purpose of the system.

Number of end users and privileged users: End Users: 5 Privileged Users: 2
In the fields above, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc.

General description of Information: Proprietary Business Information, International Agreements, Financial, Export Control, Critical Infrastructure
CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at <https://www.archives.gov/cui/registry/category-list>. (Document the CUI information types processed, stored, or transmitted by the system below).

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.

The screenshot shows the EXOSTAR Certification Assistant Standard interface. The top navigation bar includes the EXOSTAR logo, 'Certification Assistant Standard', and user information 'Certification Assistant Standard' and 'Robert Wheeling'. The main header is 'Cybersecurity Maturity Model Certification (CMMC)' with a 'Back to Cybersecurity Maturity Model Certification (CMMC) Home Page' link. A secondary navigation bar contains tabs for 'System Description', 'Stakeholders', 'System Environment', 'Policies', 'Self Assessment', 'Risk Management', 'Approval', and 'SSP/POAM'. Below this is an 'Edit' button. The main content area is divided into three sections: 'Information Owner', 'System Owner', and 'System Security Officer'. Each section has a description and a form with fields for Name, Work Phone, and Email Address.

If 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.

This screenshot shows the same EXOSTAR interface as the previous one, but in 'Save' mode. The 'Edit' button is replaced by 'Save' and 'Cancel' buttons. The 'Information Owner' section now includes a dropdown menu for 'Is this an existing user in Certification Assistant?' with 'Robert Wheeling' selected. The 'System Owner' section has a dropdown menu with 'Not an existing user' selected. The 'System Security Officer' section also has a dropdown menu with 'Not an existing user' selected. The form fields for names, addresses, and contact information are now populated with specific data.



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.

Cybersecurity NIST SP 800-171 R2 Back to Cybersecurity NIST SP 800-171 R2 Home Page

System Description Stakeholders **System Environment** Policies Self Assessment Risk Management Approval SSP/POAM

Edit

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

Upload a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.

View Document(s):

Narrative:

Include a complete and accurate listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Hardware:

#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	Reception laptop	Lenovo	PS1	Protection	Moderate	Moderate	Company	Company	receptionist

Import Hardware Inventory: [Download Import Template](#) Upload: No file chosen

Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	Microsoft Windows	Microsoft	Microsoft		2016		Protection/Processing	Moderate	Moderate	Company	Company	IT

Import Software Inventory: [Download Import Template](#) Upload: No file chosen

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.

EXOSTAR Certification Assistant Standard Certification Assistant Standard Robert Wheeling

Cybersecurity Maturity Model Certification (CMMC) Back to Cybersecurity Maturity Model Certification (CMMC) Home Page

System Description Stakeholders **System Environment** Policies Self Assessment Risk Management Approval SSP/POAM

Save Cancel

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

Upload a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.

Upload:

Document Upload:

Upload: No file chosen

Link:

Narrative:

Include a complete and accurate listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Hardware:

#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
---	------------------	------	---------	----------------	-------------	----------------	--------	-------------	-------------

Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
---	------------------	--------	----------	------	---------	--------------	----------------	-------------	----------------	--------	-------------	-------------



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.

Hardware:

#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible	
				<input type="checkbox"/> Transmission <input type="checkbox"/> Protection <input type="checkbox"/> Processing	<input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low	<input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low	<input type="radio"/> By Company <input type="radio"/> By 3rd Party	<input type="radio"/> By Company <input type="radio"/> By 3rd Party		
				<input type="button" value="Save"/>		<input type="button" value="Save & Add"/>		<input type="button" value="Delete"/>		<input type="button" value="Cancel"/>
1				Transmission,Protection	High	High	Company	Company	Todd	
Import Hardware Inventory:				<input type="button" value="Download Import Template"/>		Upload: <input type="button" value="Choose File"/> No file chosen		<input type="button" value="Import"/>		

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.

Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	Microsoft Windows	Microsoft	Microsoft		2016		Protection,Processing	Moderate	Moderate	Company	Company	IT
Import Software Inventory:				<input type="button" value="Download Import Template"/>		Upload: <input type="button" value="Choose File"/> No file chosen		<input type="button" value="Import"/>				

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.

Cybersecurity NIST SP 800-171 R2 Back to Cybersecurity NIST SP 800-171 R2 Home Page

System Description Stakeholders **System Environment** Policies Self Assessment Risk Management Approval SSP/POAM

[Edit](#)

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, coolers, printers, lab equipment, handhelds), if components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. Upload a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.

View Document(s):

Narrative:

Include a complete and accurate listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Hardware:

#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1				Transmission/Protection	High	High	Company	Company	Todd

Import Hardware Inventory: [Download Import Template](#) Upload: No file chosen [Import](#)

Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1												

Import Software Inventory: [Download Import Template](#) Upload: No file chosen [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.

Cybersecurity Maturity Model Certification (CMMC) Back to Cybersecurity Maturity Model Certification (CMMC) Home Page

System Description Stakeholders System Environment **Policies** Self Assessment Risk Management Approval SSP/POAM

Policy Upload/Link:

Policy Title:

Upload: No file chosen

-OR-

Link:

[Upload/Link File](#)

[Access Exostar PolicyPro](#)

Please ensure that you have Exostar PolicyPro. For more information, please visit <https://my.exostar.com/display/TE/PolicyPro>.

Policies:

Policy Name	File Name / URL	Linked To	Remove
311_Risk_Assessment		Asset Management - AM.2.999 Access Control - AC.1.001	X
Access Control Policy example_modified		Access Control - AC.1.002 Access Control - AC.1.001 Access Control - AC.2.999	X
http://internal.policy.acme.com	http://internal.policy.acme.com		X
https://policies.acme.com	https://policies.acme.com	Access Control - AC.1.002 Media Protection - MP.1.118 Access Control - AC.1.001	X

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

Cybersecurity Maturity Model Certification (CMMC) Back to CMMC Home Page

System Description Stakeholders System Environment **Policies** Self Assessment Risk Management Approval SSP/POAM

Policy Upload/Link:

Policy Title:

Upload: No file chosen

- OR -

Link:

Please ensure that you have Exostar PolicyPro. For more information, please visit <https://my.exostar.com/display/TE/PolicyPro>.

Policies:

Policy Name	File Name / URL	Linked To	Remove
3.11_Risk_Assessment		Asset Management - AM.2.999 Access Control - AC.1.001	<input type="button" value="X"/>
Access Control Policy example_modified		Access Control - AC.1.002 Access Control - AC.1.001 Access Control - AC.2.999	<input type="button" value="X"/>
http://internal.policyacme.com	http://internal.policyacme.com		<input type="button" value="X"/>
https://policies.acme.com	https://policies.acme.com	Access Control - AC.1.002 Media Protection - MP1.118 Access Control - AC.1.001	<input type="button" value="X"/>

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

Cybersecurity Maturity Model Certification (CMMC) Back to CMMC Home Page

System Description Stakeholders System Environment **Policies** Self Assessment Risk Management Approval SSP/POAM

Policy Upload/Link:

Policy Title:

Upload: No file chosen

- OR -

Link:

Please ensure that you have Exostar PolicyPro. For more information, please visit <https://my.exostar.com/display/TE/PolicyPro>.

Delete Policy Confirmation!

Are you sure you want to delete this policy <https://policies.acme.com>?
(There is no Undo)

Policies:

Policy Name	File Name / URL	Linked To	Remove
3.11_Risk_Assessment		Asset Management - AM.2.999 Access Control - AC.1.001	<input type="button" value="X"/>
Access Control Policy example_modified		Access Control - AC.1.002 Access Control - AC.1.001 Access Control - AC.2.999	<input type="button" value="X"/>
http://internal.policyacme.com	http://internal.policyacme.com		<input type="button" value="X"/>
https://policies.acme.com	https://policies.acme.com	Access Control - AC.1.002 Media Protection - MP1.118 Access Control - AC.1.001	<input type="button" value="X"/>

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.

The screenshot shows the EXOSTAR Certification Assistant Standard interface. The top navigation bar includes the EXOSTAR logo, the text "Certification Assistant Standard", and a user profile for "Robert Wheeling". The main content area is titled "Cybersecurity Maturity Model Certification (CMMC)" and features a navigation menu with buttons for "System Description", "Stakeholders", "System Environment", "Policies", "Self Assessment" (highlighted), "Risk Management", "Approval", and "SSP/POAM". Below the navigation menu, there are tabs for "Level 1", "Level 2", and "Level 3", with "Level 1" selected. The "Self Assessment" section is active, displaying a table of domains and their implementation status. The table has columns for "Domain", "Implemented", "Not Implemented", "Partially Implemented", and "Not Applicable".

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

The screenshot shows the "Tasks" section of the EXOSTAR Certification Assistant Standard interface. It features a table with columns for "Plan", "Task", "Assigned User", "Start Date", "Due Date", and "Status". The table is currently empty, indicating no action items are present.

Plan	Task	Assigned User	Start Date	Due Date	Status
------	------	---------------	------------	----------	--------

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.

System Description		Stakeholders		System Environment		Policies		Self Assessment		Risk Management		Approval		SSP/ POAM	
Domain: Access Control (AC) Back to Self Assessment Home Page															
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Implemented	Not Implemented	Partially Implemented	Not Applicable	View Action Items Assigned Task(s)									
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.8	Limit unsuccessful login attempts.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View									

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

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

Please describe how you have met the criteria for this Practice/Process, or any other applicable information (Implementation statement):

Comments / Activity Log:

- 06/07/21 08:20:23 AM PDT by David Wise - STATUS CHANGED via PIM Import: Implemented
- 06/07/21 07:26:44 AM PDT by David Wise - STATUS CHANGED via PIM Import: Implemented

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

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

Select Policy(s):

Please ensure that policies are uploaded into Policies section first in order to select policy

- My Policy 1
- My Policy 2
- My Policy 3

Attach Selected Policy(s)

Attached Policies:

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 versus [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

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

Artifact Upload:

Artifact Description:
Add short description of technology and/or configuration and upload the artifact(s) as proof.

Upload: No file chosen

- OR -

Link:

Attached Artifact(s):

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

Controls Comments & Log | Policy References | Assessment Guide | Consultant Feedback | Artifact Upload | **Action Items** | Workflow Tasks

What is the Action Item to be completed?

Who is going to be assigned to review and address this item?
 Willis, Andrea - Exostar UAT CA DA

Select the type of action: CMMC & NIST 800-171 POAM

When do you expect it to be completed?
 01/14/2022

SAVE

Task	Type	Assigned User	Start Date	Due Date	Status
1 Action Item - this is the follow up test :)	NIST 800-171 Only POAM	Willis, Andrea - Exostar UAT CA DA	01/06/2022	01/06/2022	Past Due!

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

Domain: Access Control (AC)		Back to Self Assessment Home Page				
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Implemented	Not Implemented	Partially Implemented	Not Applicable	View Action Item(s) Assigned Task(s)
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View

Level 1 | **Level 2** | Level 3

Domain: Access Control (AC) Back to Access Control Page

Capability: Establish system access requirements

<p>CMMC Practice ID: AC.2.005</p> <p>NIST SP 800-171.3.1.9 NIST SP 800-53 Rev 4 AC-8</p> <p>Additional References</p>	<p>Provide privacy and security notices consistent with applicable Federal Contract Information rules.</p> <p>Additional Information:</p> <p>System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via login interfaces with human users and are not required when such human interfaces do not exist. Companies may consider system use notification messages/banners displayed in multiple languages based on specific company needs and the demographics of information system users.</p> <p>This requirement references the National Archives and Records Administration's (NARA) Federal Rule 32 CFR 2002 implementing its CUI program. It applies if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Government-wide policy) requires such notices (e.g., before accessing or entering the data. This is not a common situation).</p> <p>Where to Look:</p> <ul style="list-style-type: none"> information system design documentation information system configuration settings and associated documentation information system notification messages other relevant documents or records <p>Who to Talk to:</p> <ul style="list-style-type: none"> system/network administrators system developers employees with information security responsibilities <p>Perform Test On:</p> <ul style="list-style-type: none"> automated mechanisms implementing access control policy for previous login notification 	<p>Pending Action Item(s) See Below</p> <p>Cancel Back to List</p>
--	---	---

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

What is the Action Item to be completed?

Who is going to be assigned to review and address this item?

Wheeling, Robert - Wheeling Mfg

When do you expect it to be completed?

05/25/2020

SAVE

Action Items					
Task	Assigned User	Start Date	Due Date	Status	
1 Action Item - Update and post Privacy notices	Robert Wheeling	05/25/2020	05/30/2020	New	

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.

EXOSTAR® Certification Assistant Standard

Certification Assistant Standard

Robert Wheeling

Action Item Details

Action Item - Update and post Privacy notices

Back to Previous Page

Dates & Assignment:

Start Date: 05/25/2020

Due Date: 05/30/2020

Assigned to: Wheeling, Robert

Response:

Previous Task/Control Notes:

05/25/20 04:07:34 PM PDF by Robert Wheeling - STATUS CHANGED via PIM Import: Not Implemented

Remove this Task

Upload/Link Files

Close this Task

Cancel **SAVE**

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

Cybersecurity NIST SP 800-171 R2 Back to Cybersecurity NIST SP 800-171 R2 Home Page

System Description | Stakeholders | System Environment | Policies | **Self Assessment** | Risk Management | Approval | SSP/POAM

Self Assessment Print Self Assessment | Print Open Action Items

Domain		Implemented	Not Implemented	Partially Implemented	Not Applicable
AC - Access Control	21 / 23 ▲	20	1	1	1
AU - Audit and Accountability	9 / 9 ✓	9	0	0	0

Tab 6 – Workflow Tasks

Controls Comments & Log | Policy References | Assessment Guide | Consultant Feedback | Artifact Upload | Action Items | **Workflow Tasks**

What is the Workflow Task to be scheduled?

Who is going to be assigned to complete this task?

Wills, Andrea - Exostar UAT CA OA ▼

SAVE

Open Assigned Tasks

Task	Type	Assigned User	Start Date	Due Date	Status
1 Scheduled Action Item - this is the daily work flow item	Workflow	Wills, Andrea - Exostar UAT CA 1	01/07/2022	01/07/2022	Past Due!
2 Scheduled Action Item - this is the daily work flow item	Workflow	Wills, Andrea - Exostar UAT CA 1	01/10/2022	01/10/2022	Past Due!
3 Scheduled Action Item - this is the daily work flow item	Workflow	Wills, Andrea - Exostar UAT CA 1	01/13/2022	01/13/2022	Past Due!

Defined Recurring Tasks

Task	Schedule Type	Assigned User	Schedule Details
1 Scheduled Action Item - this is the daily work flow item	Daily	Andrea Wills	Includes Weekends ✖

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.

Controls Comments & Log | Policy References | Assessment Guide | Consultant Feedback | Artifact Upload | Action Items | **Workflow Tasks**

What is the Workflow Task to be scheduled?

Who is going to be assigned to complete this task?

Wills, Andrea - Exostar UAT CA OA ▼

SAVE

Select Schedule:

- Daily
- Weekly
- Monthly
- Quarterly
- Yearly
- Specific Date

Select Day(s) of the Week:

- Sunday Monday
- Tuesday Wednesday
- Thursday Friday
- Saturday

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.

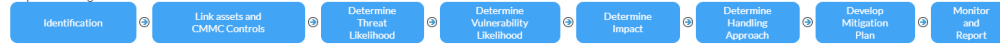
Updating each active task is the same as an action item (POAMs) as shown below.

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

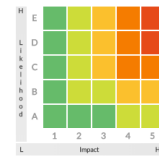
Domain: Access Control (AC)		Back to Self Assessment Home Page				
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Implemented	Not Implemented	Partially Implemented	Not Applicable	View (Action Items) Assign Task(s)
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View

Risk Management Tab

Steps in creating a risk item



Risk Inventory												
#	Risk Title	Manager	Category	Threat Likelihood	Vulnerability Likelihood	Overall Likelihood	Risk Impact	Risk Rating	Linked Assets	Linked Controls	Risk Handling	Open Actions
View CMMC Risk Management Requirements To add new risk items, click here --> Add Risk												



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.

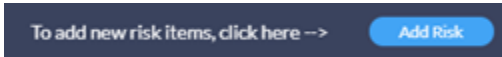
Notes for risk cube:

- 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.

CMMC Risk Management Requirements:		
Capability	Level	Practice
CMMC Identify and analyze risk	2	<p>SP12-040 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Federal Contract Information.</p> <p>SP12-042 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.</p>
	3	<p>SP12-044 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk management criteria.</p>
	4	<p>SP12-046 Catalog and periodically update threat profiles and adversary TTPs.</p> <p>SP12-030 Employ threat intelligence to inform the development of the system and security architecture, selection of security solutions, monitoring, threat hunting, and response and recovery activities.</p> <p>SP12-032 Perform counter-unsanctioned ports available across perimeter network boundaries over the organization relevant network boundaries and other organizationally defined boundaries.</p>
	2	<p>SP12-040 Remediate vulnerabilities in accordance with risk assessments.</p>

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

Identification

Risk Title:

Risk Manager:

Category:

Internal - originates within the company

External - originates outside the company

External Supply Chain - originates within the supplier network

Need Assistance?
 NIST Cybersecurity for Small Business, the Fundamentals
<https://www.nist.gov/document/nistsmallbusinessfundamentalsjuly2019pptx>

SAVE & Next Step

Cancel

Additional resources for cybersecurity "threat" Identification:

Threat - Reference NIST 800-30 R1. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Common Cybersecurity Threats
 (Access the links to the right for more assistance with information security threat identification)
 (Provided as reference only. Each company needs to determine threats to their information security.)

- Phishing** - A social engineering attack involving trickery that's designed to gain access to systems or steal data. Example - an email is sent to company employees causing some sort of urgency to respond or click on a link. Clicking on the link causes a download of malware to your network. A variant of Phishing is called Spear Phishing which is a targeted campaign toward a specific group or individual within a company.
- Ransomware** - A type of software that can encrypt or lock data behind a secret key or passphrase. Without the code, data and network are inaccessible.
- Environmental** - A natural disaster such as fire, hurricane, tornado, etc. can cause damage or loss to computer hardware and systems leaving information inaccessible.
- Hacking** - When someone stages an attack on your network or the systems you use. Typically the hacking attack will occur without anyone ever setting foot in your office or on your property. They will utilize access via the internet or on your own network to go after some aspect of your environment. Hacking can also occur when a trusted employee or visitor to our physical environment abuses that trust to illegally access other areas of the business.

Risk Title - What is the "threat"? Short succinct title.

Risk Manager - The person responsible for managing the risk.

Helpful Resources

- Cybersecurity for Small Business, the Fundamentals
<https://www.nist.gov/document/nistsmallbusinessfundamentalsjuly2019pptx>
- The 5 Most Common Cybersecurity Threats to Manufacturers
<https://www.nist.gov/blog/manufacturing-innovation-blog/5-most-common-cybersecurity-threats-manufacturers>
- Guide for Conducting Risk Assessments
<https://csirc.nist.gov/publications/detail/sp/800-30/rev-1/final>
- IT Asset Management
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf>
- Cybersecurity Planning Guide
<https://transition.fcc.gov/cyber/cyberplanner.pdf>

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)

NOTE: Each business is different and the relationship between business assets and risk items, and CMMC Controls and risk items are business specific and should be determined by subject matter experts with knowledge pertaining the specific business.

CMMC Practice RM.2.141: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Federal Contract Information.

1. For the identified risk, identify which asset(s) identified in the System Environment exercise that could be exploited or are vulnerable to the threat.
2. For the identified risk, identify which CMMC Control Domain associated with the identified threat or vulnerability.

Helpful Resources

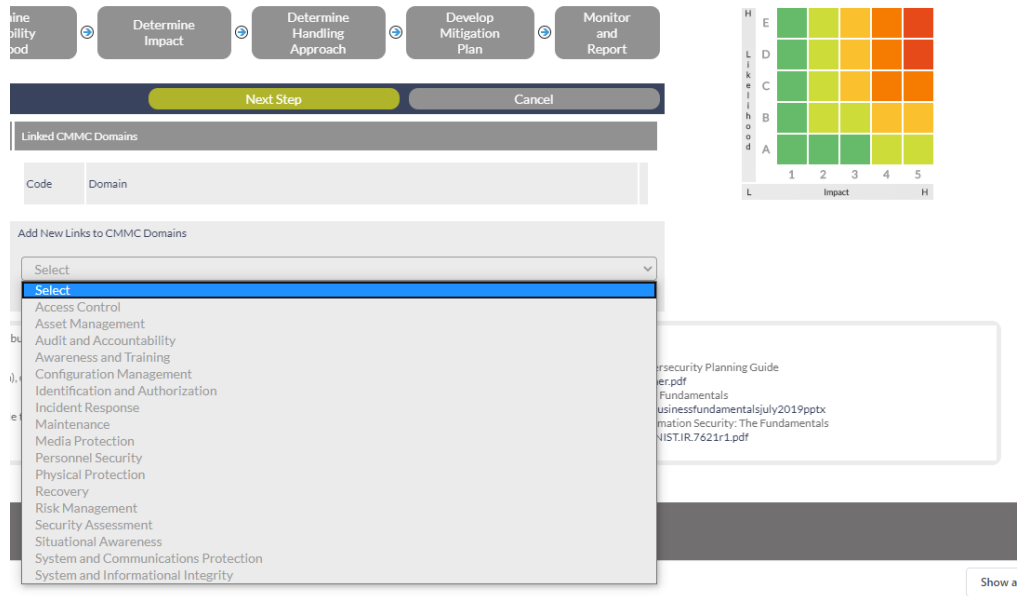
- Federal Communication Commission, Cybersecurity Planning Guide
<https://transition.fcc.gov/cyber/cyberplanner.pdf>
- NIST Cybersecurity for Small Business, the Fundamentals
<https://www.nist.gov/document/nistsmallbusinessfundamentalsjuly2019pbx>
- NIST 7623, Revision 1, Small Business Information Security: The Fundamentals
<https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7623r1.pdf>

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.

Threat Likelihood Assessment (How likely is the threat or threat-event to happen?)

NIST SP 800-30 R1 - Formal description and evaluation of threat to an information system. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

<input type="radio"/>	Very High	Error, accident, event or act of nature is almost certain to occur
<input type="radio"/>	High	Error, accident, event or act of nature is highly likely to occur
<input type="radio"/>	Moderate	Error, accident, event or act of nature is somewhat likely to occur
<input type="radio"/>	Low	Error, accident, event or act of nature is unlikely to occur
<input type="radio"/>	Very Low	Error, accident, event or act of nature is highly unlikely to occur

Please give a short explanation as to why the selection was made. The information is useful during risk meetings to support the Threat assessment.

SAVE & Next Step **Cancel**

NOTE: Each business is different and considerations for determining a threat assessment should be specific to the company and determined by subject matter experts with knowledge pertaining the specific business. Determining the threat assessment is not an exact science; input from subject matter experts, company employees or outside consultants are ways to gather the necessary information needed to make a logical decision. For this exercise, transform the threat descriptor into a question and see what answer is derived. Example - Do we believe the "[threat name]" is certain to occur? Ask the question for each level and decide on the threat level. After the threat level has been decided, provide a brief justification as to "Why" the threat level was selected. Example - The level is high due to numerous phishing attacks have been discovered over the last few months.

Helpful Resources

- Cybersecurity for Small Business, the Fundamentals <https://www.nist.gov/document/nist-small-business-fundamentals-july-2019-ppt>
- NIST SP 800-30 R1, Guide for Conducting Risk Assessments <https://src.nist.gov/publications/detail/sp/800-30/rev-1/final>

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.

Vulnerability Likelihood Assessment (If the Threat were enacted, how likely would a weakness be exploited?)

(NIST 800-30 R1) Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

<input type="radio"/>	Very High	Very high concern. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
<input type="radio"/>	High	High concern. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
<input type="radio"/>	Moderate	Moderate concern. Relevant security control or other remediation is partially implemented and somewhat effective.
<input type="radio"/>	Low	Minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
<input type="radio"/>	Very Low	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

Please give a short explanation as to why the selection was made. The information is useful during risk meetings to support the Vulnerability assessment.
Assistant: Identified vulnerabilities will be addressed in the mitigation plan.

SAVE & Next Step

Cancel

NOTE: Each business is different and considerations for determining a vulnerability assessment should be specific to the company and determined by subject matter experts with knowledge pertaining to the specific business. There may be more than one vulnerability identified for a given risk (threat).

The primary purpose of vulnerability assessments is to understand the nature and degree to which organizations, mission/business processes, and information systems are vulnerable to threat sources identified during the Threat identification process. 1. Determining the vulnerability assessment is not an exact science; input from subject matter experts, company employees or outside consultants are ways to gather the necessary information needed to make a logical decision.

Example - (High) A recent IT audit found that there is a significant backlog of software patches. Keeping up with software patches help protect IT environments from threats.

Helpful Resources

- NIST SP 800-30 R1, Guide for Conducting Risk Assessments
<https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
- Cybersecurity for Small Business, the Fundamentals
<https://www.nist.gov/document/nist-small-business-fundamentals-july-2019-pptx>
- Information about threats and common vulnerabilities can be found through your local InfraGard chapter [InfraGard], [US-CERT], your local SCORER chapter, hardware or software vendor announcements, your local police department and many other places (e.g., the National Vulnerability Database [NVD]).

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.

Consequence/Impact Assessment (If the threat occurred and the vulnerability exploited, estimate the consequence)

NIST SP 800-30 Table H-3

<input type="radio"/>	Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
<input type="radio"/>	High	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
<input type="radio"/>	Moderate	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.
<input type="radio"/>	Low	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.
<input type="radio"/>	Very Low	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Please give a short explanation as to why the selection was made. The information is useful during risk meetings to support the Consequence/Impact assessment.

[SAVE & Next Step](#) [Cancel](#)

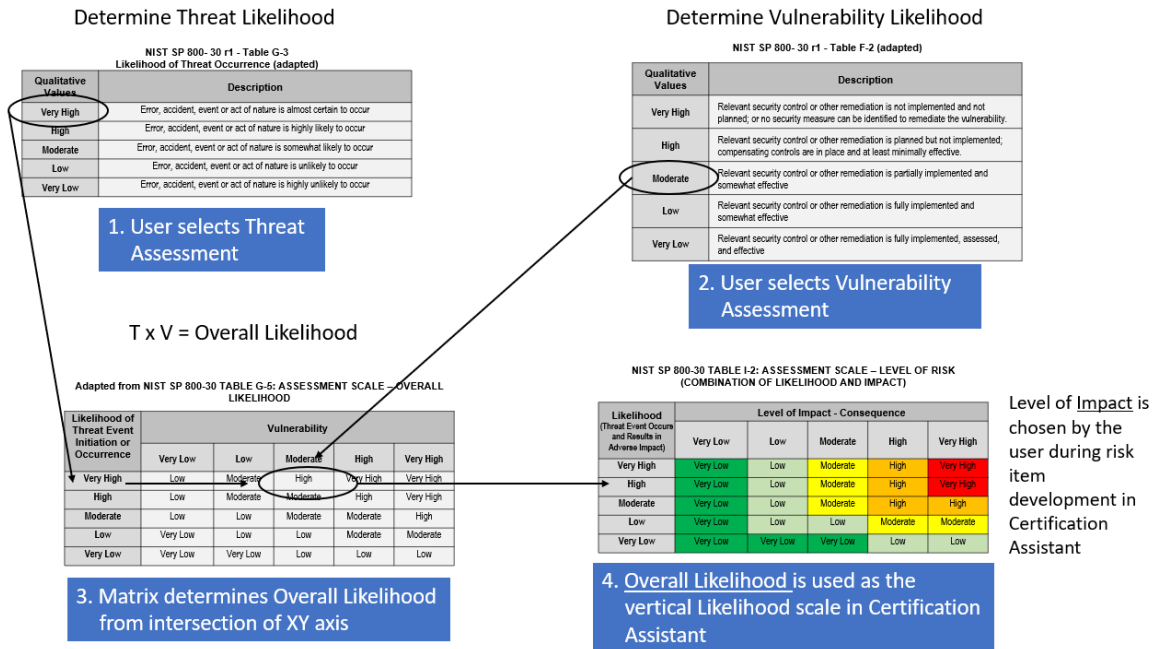
HIGH - A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

MODERATE - A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

LOW - A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

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.

NOTE: Each business is different and considerations for developing a risk mitigation plan should be specific to the company and determined by subject matter experts with knowledge pertaining the specific business.

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (NIST SP 800-30 B1)

Answer the question, "What can be done to reduce the current risk level?" Having more than one mitigation activity for single risk may be necessary.

Mitigation Activity Examples: Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.1

Helpful Resources

- Federal Communication Commission, Cybersecurity Planning Guide <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- NIST Cybersecurity for Small Business, the Fundamentals <https://www.nist.gov/document/nistsmallbusinessfundamentalsjuly2019pptx>
- NIST Manufacturing Extension Partnership (MEP) <https://www.nist.gov/mep/cybersecurity-resources-manufacturers/where-start>
- NIST 7621 Revision 1, Small Business Information Security: The Fundamentals <https://nvlpubs.nist.gov/nistpubs/fr/2016/nist1k.7621r1.pdf>
- NIST SP 800-39, Managing Information Security Risk <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- NIST Small Business Cybersecurity Corner <https://www.nist.gov/it/smallbusinesscyber/planning-guides>
- NIST Cybersecurity Website <https://www.nist.gov/topics/cybersecurity>
- NIST SP 1800-5, IT Asset Management <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf>

Identification → Link assets and CMMC Controls → Determine Threat Likelihood → Determine Vulnerability Likelihood → Determine Impact → Determine Handling Approach → **Develop Mitigation Plan** → Monitor and Report

Risk Mitigation Action Items New Mitigation Action Return to Risk Home

What is the Mitigation Action Item to be completed?

Who is going to be assigned to review and address this item?
 Wise, David - CEO

When do you expect it to be completed?
 06/01/2020

SAVE

NOTE: Each business is different and considerations for developing a risk mitigation plan should be specific to the company and determined by subject matter experts with knowledge pertaining the specific business.
 Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (NIST SP 800-30 R1)
 Answer the question, "What can be done to reduce the current risk level?" A A. Having more than one mitigation activity for single risk may be necessary.
 Mitigation Activity Examples: Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.3

Helpful Resources

- Federal Communication Commission, Cybersecurity Planning Guide <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- NIST Cybersecurity for Small Business, the Fundamentals <https://www.nist.gov/document/nist-small-business-fundamentals-july-2019.pptx>
- NIST Manufacturing Extension Partnership (MEP) <https://www.nist.gov/mep/cybersecurity-resources-manufacturers/where-start>
- NIST 7621 Revision 1, Small Business Information Security: The Fundamentals <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf>
- NIST SP 800-39, Managing Information Security Risk <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- NIST Small Business Cybersecurity Corner <https://www.nist.gov/it/smallbusinesscyber/planning-guides>
- NIST Cybersecurity Website <https://www.nist.gov/topics/cybersecurity>
- NIST SP 1800-5, IT Asset Management <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf>

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

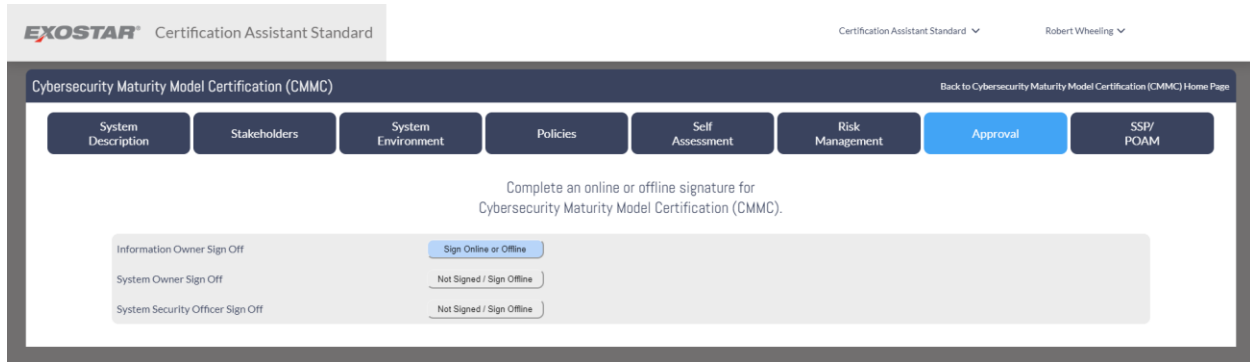
(Also known as Communication and Sharing)

Maintaining Risk Assessments

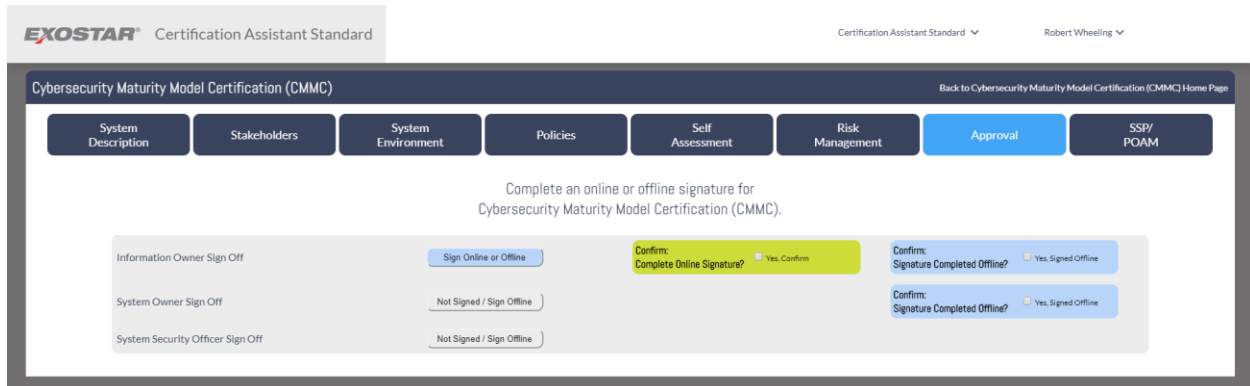
- i. Determine the appropriate method (e.g., executive briefing, risk assessment report, or dashboard) to communicate risk assessment results.
- ii. Communicate risk assessment results to designated organizational stakeholders.
- iii. Share the risk assessment results and supporting evidence in accordance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

Approval Tab

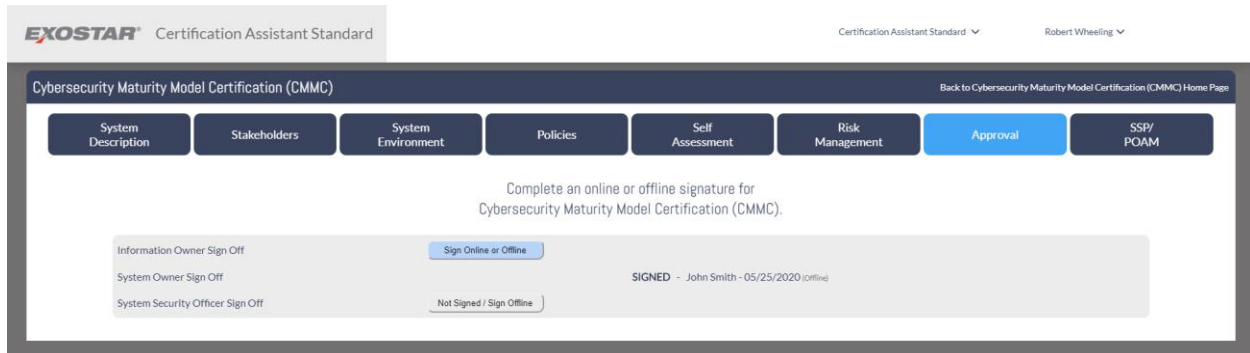
After all the content has been added to the tabs, the Approval tab can be used to sign the content either online or offline. Online signatures can be accomplished by the user if their name was linked to the information on the Stakeholders tab. If online signature is available, the blue Sign Online or 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.

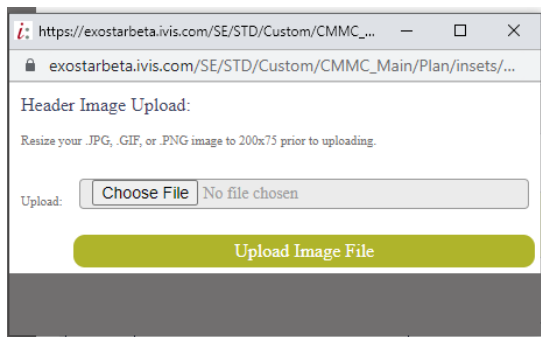


SSP/POAM Tab

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.

Cybersecurity NIST SP 800-171 R2 Back to Cybersecurity NIST SP 800-171 R2 Home Page

System Description | Stakeholders | System Environment | Policies | Self Assessment | Risk Management | Approval | **SSP/POAM**

SSP & POAM

Generate and View SSP & POAM



Add your logo to your SSP and POAM report

SSP						POAM				
Generate NIST 800-171 SSP						Generate NIST 800-171 POAM				
#	NIST 800-171 SSP Generated By	Date	DoD Assessment Methodology Basic Assessment Score	DoD Assessment Methodology Report	Approvals	#	NIST 800-171 POAM Generated By	Date	Approvals	NIST 800-171 POAM
1	Andrea Willis	05/14/2022 09:21	#F	View	11/09/2021 11/09/2021 11/09/2021	1	Christine Parsons	05/12/2022 07:22	11/09/2021 11/09/2021 11/09/2021	View

Cybersecurity NIST SP 800-171 R2 Back to Cybersecurity NIST SP 800-171 R2 Home Page

System Description | Stakeholders | System Environment | Policies | Self Assessment | Risk Management | Approval | **SSP/POAM**

SSP & POAM

Generate and View SSP & POAM

Delete SSP/POAM Logo Confirmation!

Are you sure you want to delete the current header image?
(There is no Undo!)

SSP						POAM			
Generate NIST 800-171 SSP						Generate NIST 800-171 POAM			


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.



System Security Plan
05/25/2020

1. SYSTEM IDENTIFICATION

1.1 System Name: Wheeling Life Internal Network

1.1.1 System Categorization: SC network information - (confidentiality, NCOB/MATE), integrity, NCOB/MATE, (availability, COWE)

1.1.2 System Unique Identifier: WheelingLife

1.2 Responsible Organization: 100 Main St
Phoenix, AZ 85001
USA

1.2.1 Information Owner: Robert Wheeling
100 Main St
Phoenix, AZ 85001
USA
Work Phone: 480-235-1234 x331
Email Address: rhwheeling@wheelinglife.com

1.2 System Owner: John Smith
100 Main St
Phoenix, AZ 85001
USA
Work Phone: 480-235-1234 x331
Email Address: jsmith@wheelinglife.com

1.2.3 System Security Officer: Nancy Jones
100 Main St
Phoenix, AZ 85001
USA
Work Phone: 480-235-1234 x331
Email Address: njones@wheelinglife.com

1.3 General Purpose of the System: Internal user support for account management, engineering, manufacturing and distribution.

1.3.1 Number of End Users and Privileged Users:

Number of Users	Number of Administrators/ Privileged Users
3	2

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.

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

SSP

[Generate 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

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	Task	Assigned User	Start Date	Due Date	Status
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 PM Import, Not Implemented

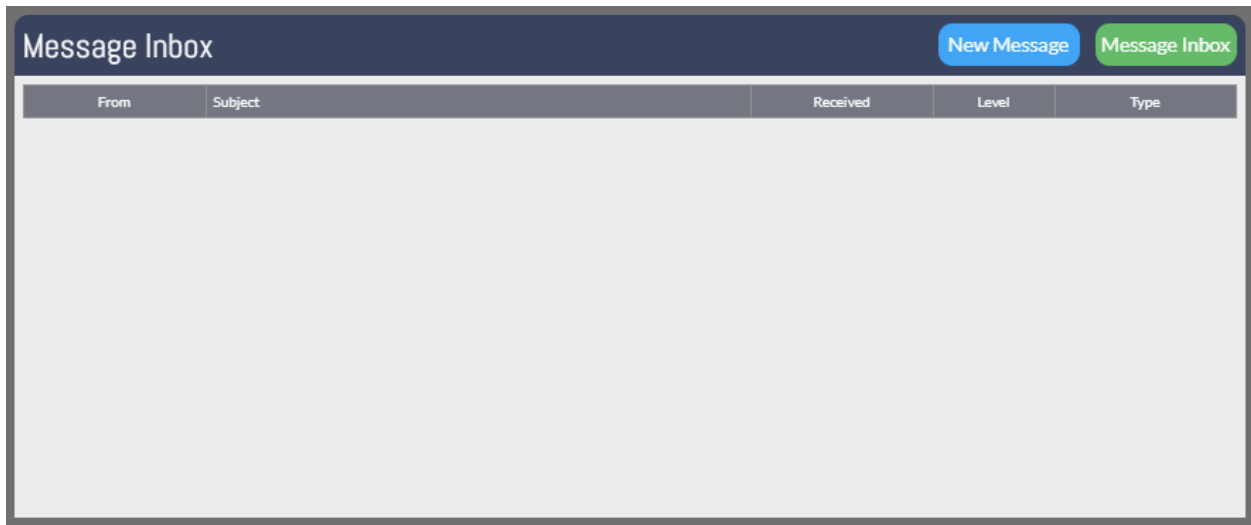
Certification Assistant Messaging

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 screenshot shows a 'New Message' form with the following fields and options:

- To*:** A dropdown menu with 'McInfo, Steven - DIB Consulting' selected.
- Message Type:** A dropdown menu with 'Message' selected.
- Subject*:** An empty text input field.
- Message*:** A large empty text area for the message content.
- Level*:** Radio buttons for 'Normal' (selected), 'Important', and 'Critical'.
- Upload:** Two buttons: 'Choose Files' and 'No f...osen'.
- Buttons:** 'Cancel' and 'Send' buttons at the bottom.

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.

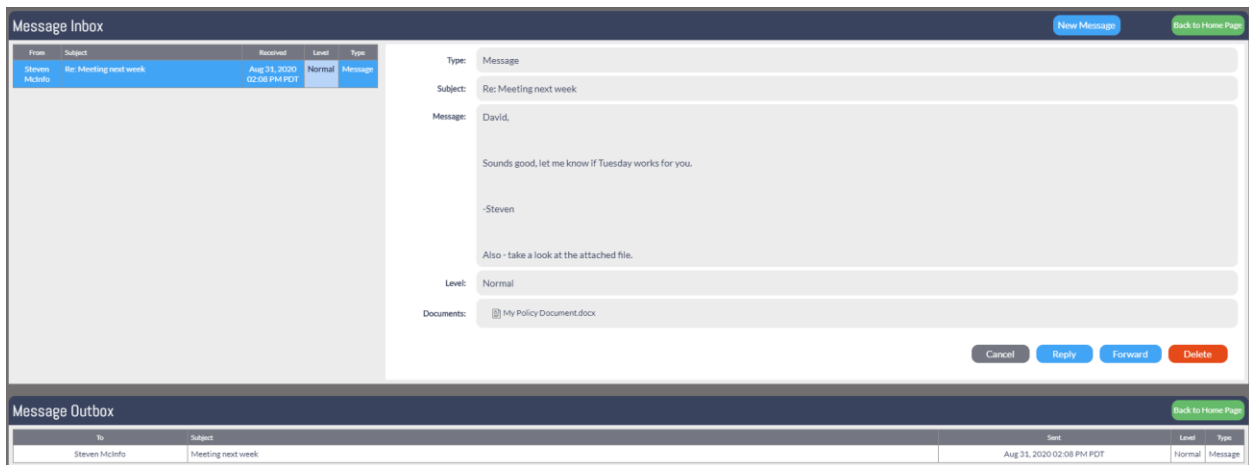
New messages will be highlighted blue and always at the top of the list.



The screenshot shows a 'Message Inbox' header with 'New Message' and 'Message Inbox' buttons. Below is a table with one row highlighted in blue:

From	Subject	Received	Level	Type
Steven McInfo	Re: Meeting next week	Aug 31, 2020 02:08 PM PDT	Normal	Message

Click on the message to view.



The screenshot shows a 'Message Inbox' header with 'New Message' and 'Back to Home Page' buttons. Below is a table with one row highlighted in blue:

From	Subject	Received	Level	Type
Steven McInfo	Re: Meeting next week	Aug 31, 2020 02:08 PM PDT	Normal	Message

Message details:

- Type: Message
- Subject: Re: Meeting next week
- Message: David,
Sounds good, let me know if Tuesday works for you.
-Steven
Also - take a look at the attached file.
- Level: Normal
- Documents: My Policy Document.docx

Buttons: Cancel, Reply, Forward, Delete

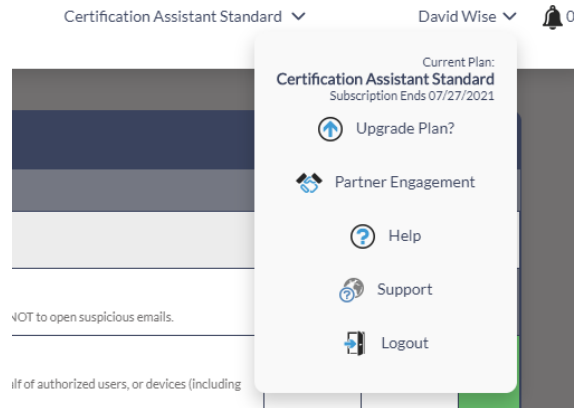
Message Outbox header with 'Back to Home Page' button:

To	Subject	Sent	Level	Type
Steven McInfo	Meeting next week	Aug 31, 2020 02:08 PM PDT	Normal	Message

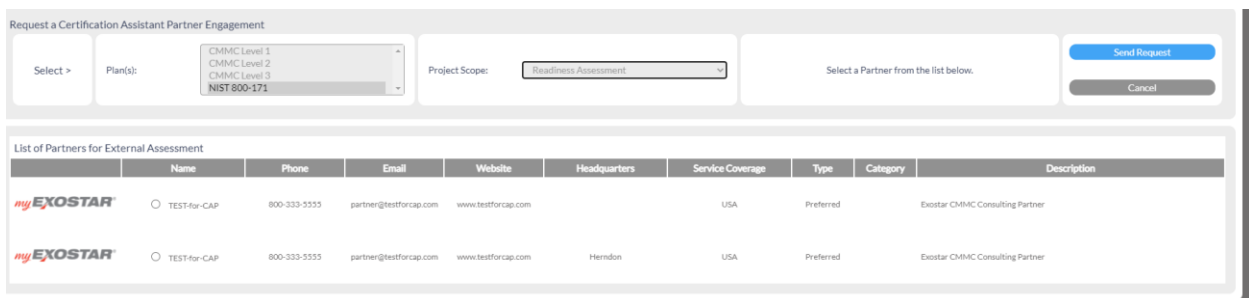
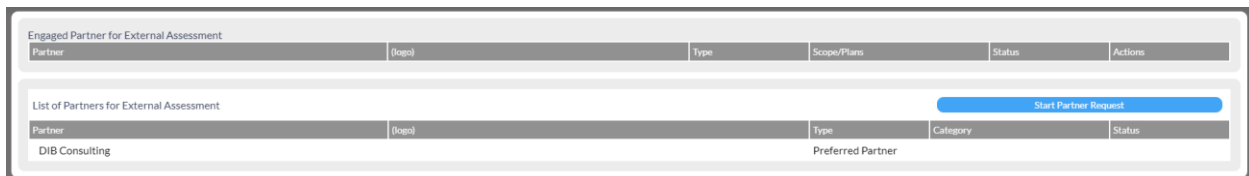
To reply to this message, click on the Reply button and Send when your message is complete. Similarly, to Forward to another user, click on Forward and Send when your message is complete.

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:

Partner Engagement Request Confirmation!

The engagement request for **Readiness Assessment** regarding **CMMC Level 3** will be sent to the selected partner. Partner will be provided your contact information and contact you to discuss business and legal terms soon. Once the selected partner accepts your engagement request, you will be notified of Partner's acceptance. Partner will request access to your Certification Assistant.

Do you want to proceed?

(logo)	Type	Scope/Plans
--------	------	-------------

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.

Message Inbox					New Message	Message Inbox
From	Subject	Received	Level	Type		
Steven McInfo	Access Request Notification	Aug 31, 2020 04:08 PM PDT	Important	Message		

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

Partner Engagement Access Request!

You are about to approve the access request from **DIB Consulting**.
The partner will access all the data of your assessment and verify your assessment if necessary.
Please ensure that the business and legal terms be agreed before approval.

Do you want to approve this access request?

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.



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