Certification Assistant Lite User Guide

January 2022

Contents

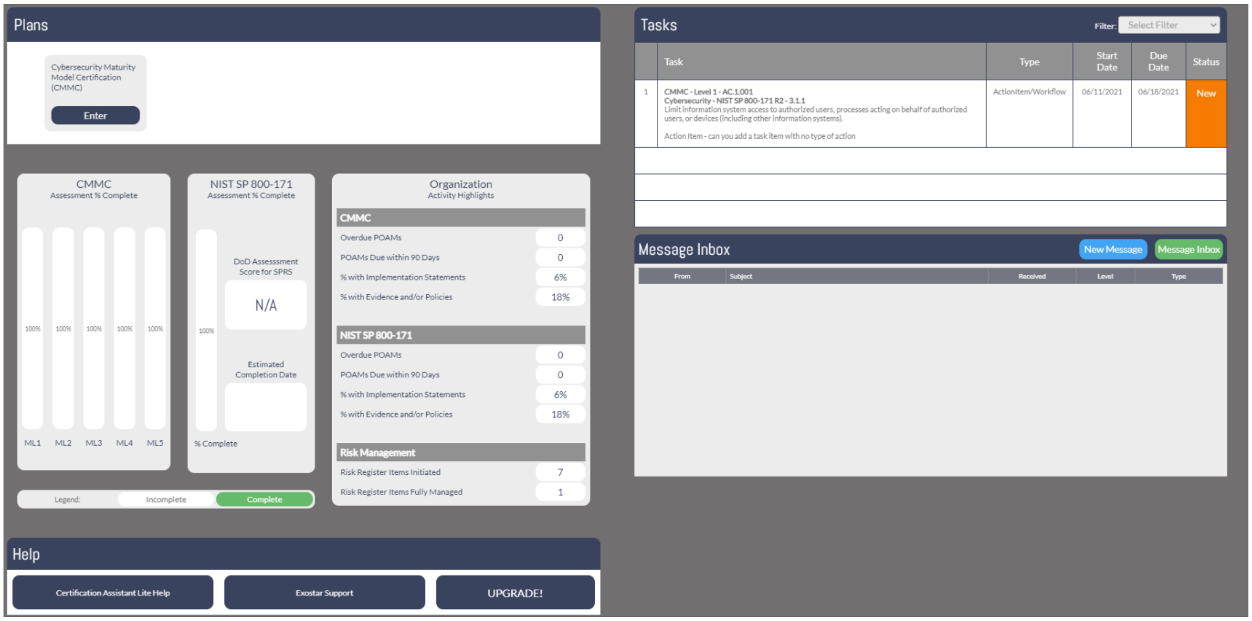
DOCUMENT VERSIONS

Version	Impacts	Date
Certification Assistant		Pre-June 2021
CA 1.4	1.4 includes: • Dashboard redesign • Update to Individual Self-Assessment: ○ New Tab structure ▪ Controls Comments and Logs (Implementation Statement ▪ Policy References ▪ Assessment guide ▪ Artifact Upload ▪ Action Items • Updates to Policies • Added Scope to System Description	June 2021
CA 1.5	No changes to Lite	August 2021
CA 1.6	The following changes have been implemented for Lite: • Ability to import both Software and Hardware inventory on System Environment tab • Improved Usability ▪ Navigation from within individual controls ▪ Decision a control from Domain Dashboard • Ability to create workflow items on a schedule i.e. daily, weekly, monthly, quarterly or yearly basis • Ability to share documents between partner and you	January 2022

Certification Assistant Lite 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.



Organization
Activity Highlights

CMMC	
Overdue POAMs	0
POAMs Due within 90 Days	0
% with Implementation Statements	6%
% with Evidence and/or Policies	18%
NIST SP 800-171	
Overdue POAMs	0
POAMs Due within 90 Days	0
% with Implementation Statements	6%
% with Evidence and/or Policies	18%
Risk Management	
Risk Register Items Initiated	7
Risk Register Items Fully Managed	1

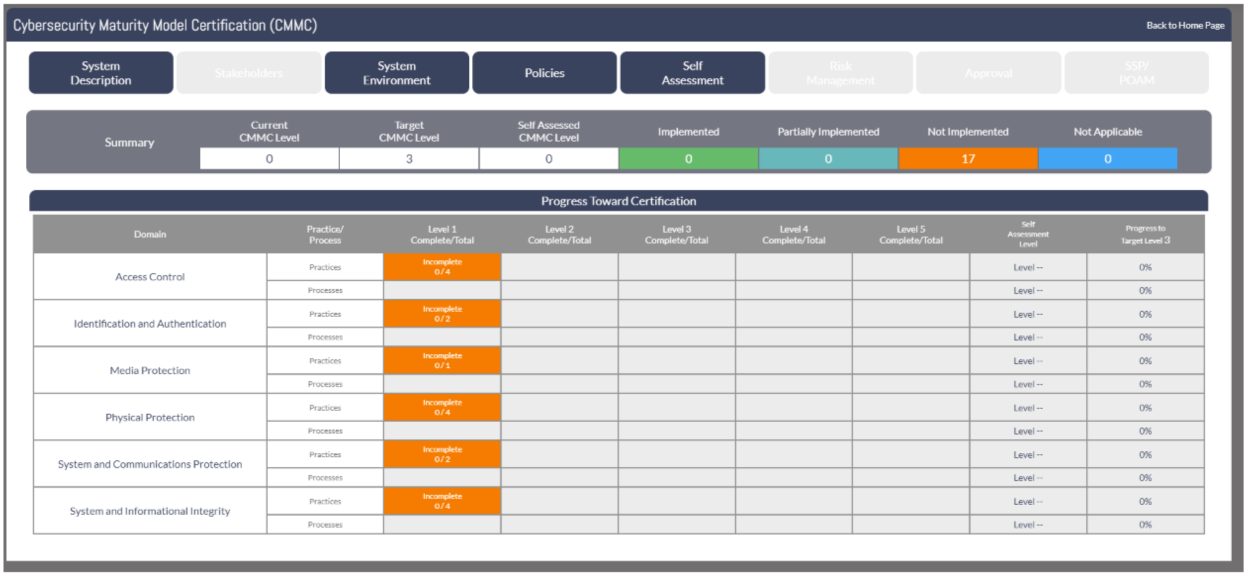
	Task	Type	Start Date	Due Date	Status
1	**CMMC - Level 1 - AC.1.001** **Cybersecurity - NIST SP 800-171 R2 - 3.1.1** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Action Item - can you add a task item with no type of action	ActionItem/Workflow	06/11/2021	06/18/2021	New

From	Subject	Received	Level	Type

To access the CMMC program details, click on the Cybersecurity Maturity Model Certification (CMMC) button.
If there are Actions Items available, click on the Task Name to access the task details page.

Cybersecurity Maturity Model Certification (CMMC) Home Page

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

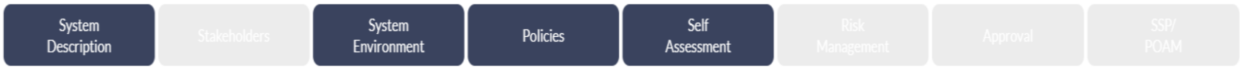


Summary	Current CMMC Level	Target CMMC Level	Self Assessed CMMC Level	Implemented	Partially Implemented	Not Implemented	Not Applicable
	0	3	0	0	0	17	0

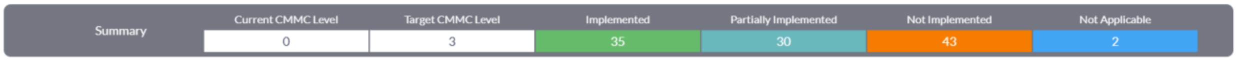
Progress Toward Certification

Domain	Practice/ Process	Level 1 Complete/Total	Level 2 Complete/Total	Level 3 Complete/Total	Level 4 Complete/Total	Level 5 Complete/Total	Self Assessment Level	Progress to Target Level 3
Access Control	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%
Identification and Authentication	Practices	Incomplete 0 / 2					Level --	0%
	Processes						Level --	0%
Media Protection	Practices	Incomplete 0 / 1					Level --	0%
	Processes						Level --	0%
Physical Protection	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%
System and Communications Protection	Practices	Incomplete 0 / 2					Level --	0%
	Processes						Level --	0%
System and Informational Integrity	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%

The Tab Toolbar is how you will navigate through the system to complete each section. The buttons that are greyed out are features available in Certification Assistant Standard and Premium. Use the Upgrade links to view details about these versions.

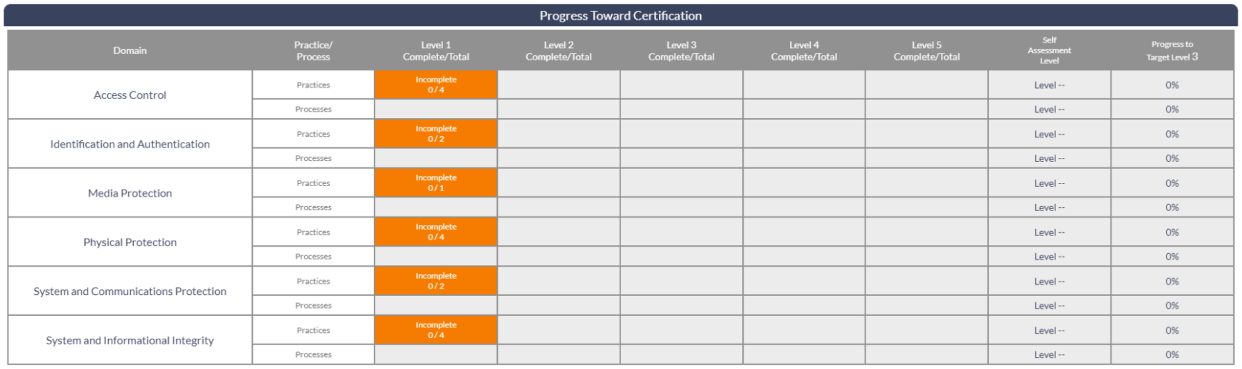


The Summary bar shows your current CMMC Level, Target CMMC Level, Self-Assessed CMMC Level and the number of controls in each level of implementation; Implemented, Partially Implemented, Not Implemented and Not Applicable.



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

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



Progress Toward Certification

Domain	Practice/ Process	Level 1 Complete/Total	Level 2 Complete/Total	Level 3 Complete/Total	Level 4 Complete/Total	Level 5 Complete/Total	Self Assessment Level	Progress to Target Level 3
Access Control	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%
Identification and Authentication	Practices	Incomplete 0 / 2					Level --	0%
	Processes						Level --	0%
Media Protection	Practices	Incomplete 0 / 1					Level --	0%
	Processes						Level --	0%
Physical Protection	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%
System and Communications Protection	Practices	Incomplete 0 / 2					Level --	0%
	Processes						Level --	0%
System and Informational Integrity	Practices	Incomplete 0 / 4					Level --	0%
	Processes						Level --	0%

How to read the chart – using Access Control as an example:

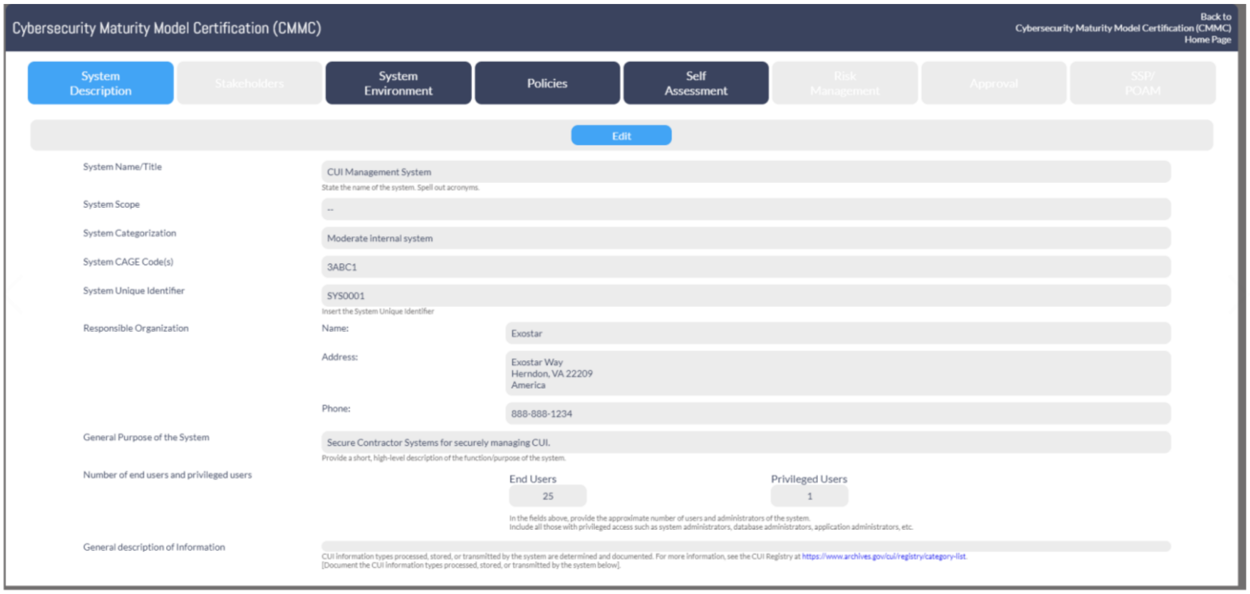
- There are Practices and Processes in each CMMC domain from Level 2 on.
  - There are limited practices and no processes in Level 1, therefore the chart shows a grey cell with no data. As a Certification Assistant Lite user, you will only have access to Level 1.
- When a Level contains 0 completed controls, it will show orange and 0 out of 2 (for example) and 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.

System Description Tab

The System Description tab is used to start the information gathering required for a System Security Plan or SSP report.

NOTE: Lite access does not allow for generation of a SSP. You would need to upgrade to Standard or Premium.

Click on the 'Edit' button to enter edit mode and complete the form.

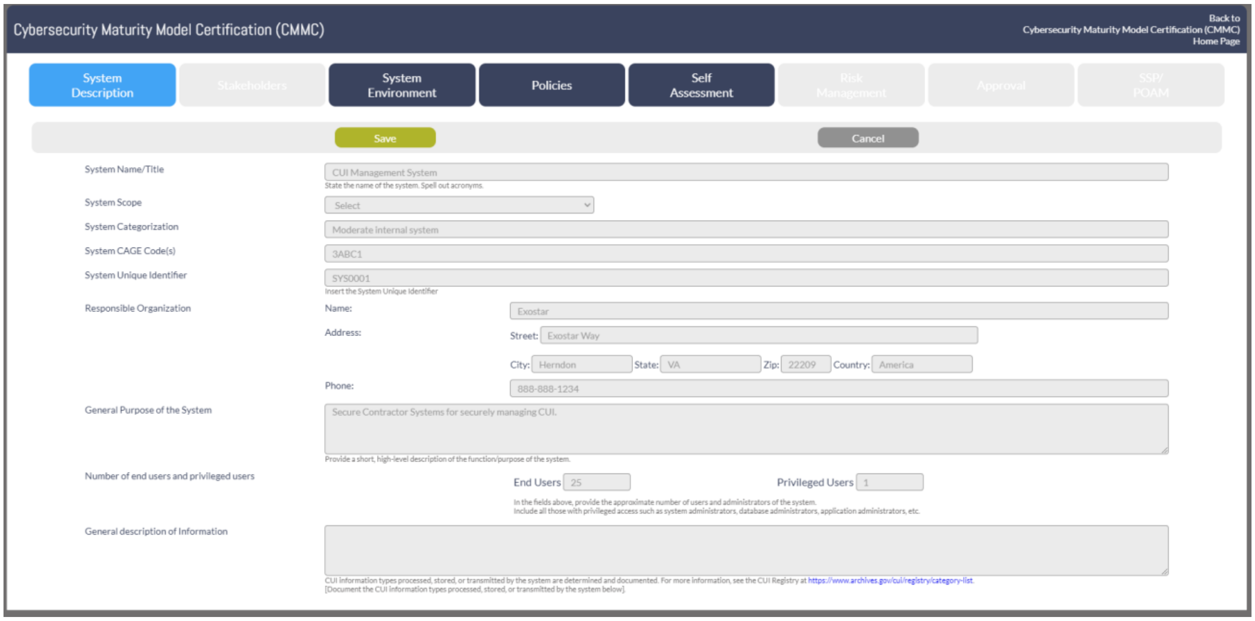

Cybersecurity Maturity Model Certification (CMMC)
Back to Cybersecurity Maturity Model Certification (CMMC) Home Page
System Description
Stakeholders
System Environment
Policies
Self Assessment
Risk Management
Approval
SSP/ POAM
Edit

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. [Document the CUI information types processed, stored, or transmitted by the system below].	

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.


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: CUI Management System
State the name of the system. Spell out acronyms.

System Scope: Select

System Categorization: Moderate internal system

System CAGE Code(s): 3ABC1

System Unique Identifier: SYS0001
Insert the System Unique Identifier

Responsible Organization
Name: Exostar
Address:
Street: Exostar Way
City: Herndon State: VA Zip: 22209 Country: America
Phone: 888-888-1234

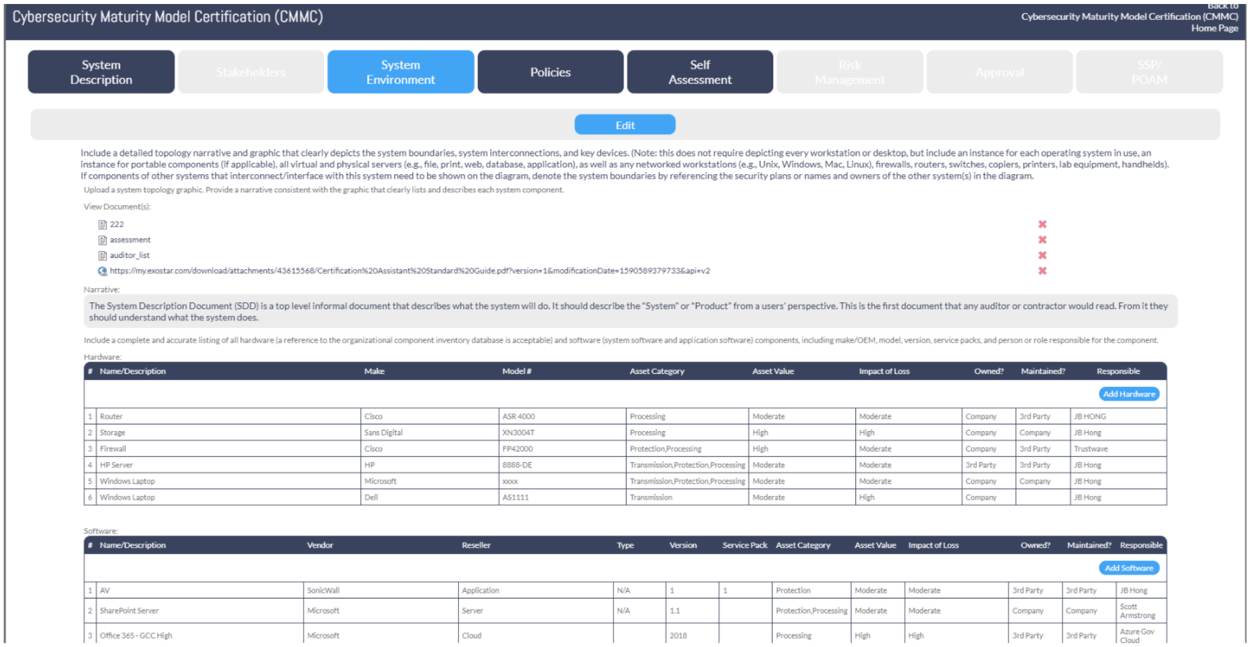
General Purpose of the System: Secure Contractor Systems for securely managing CUI.
Provide a short, high-level description of the function/purpose of the system.

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.
[Document the CUI information types processed, stored, or transmitted by the system below].

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.



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):
- 222 ✖
- assessment ✖
- auditor_list ✖
- https://my.exostar.com/download/attachments/43615568/Certification%20Assistant%20Standard%20Guide.pdf?version=1&modificationDate=1590589379733&api=v2 ✖

Narrative:
The System Description Document (SDD) is a top level informal document that describes what the system will do. It should describe the "System" or "Product" from a users' perspective. This is the first document that any auditor or contractor would read. From it they should understand what the system does.

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:

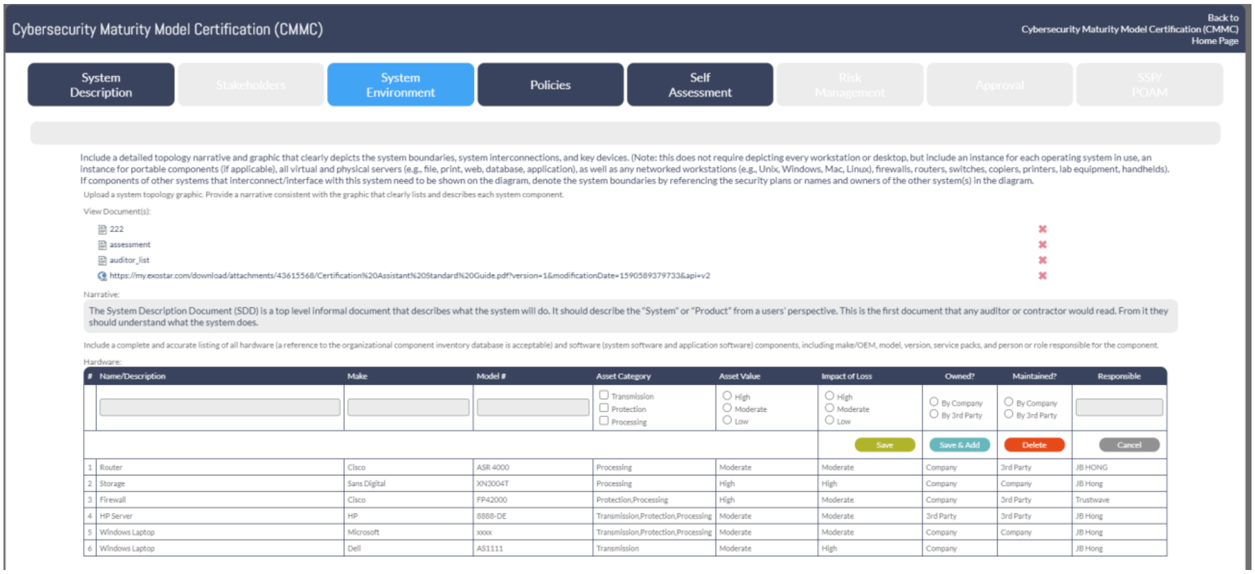
#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	Router	Cisco	ASR 4000	Processing	Moderate	Moderate	Company	3rd Party	JB HONG
2	Storage	Sans Digital	XN3004T	Processing	High	High	Company	Company	JB Hong
3	Firewall	Cisco	FP42000	Protection,Processing	High	Moderate	Company	3rd Party	Trustwave
4	HP Server	HP	8888-DE	Transmission,Protection,Processing	Moderate	Moderate	3rd Party	3rd Party	JB Hong
5	Windows Laptop	Microsoft	xxxx	Transmission,Protection,Processing	Moderate	Moderate	Company	Company	JB Hong
6	Windows Laptop	Dell	AS1111	Transmission	Moderate	High	Company		JB Hong

Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	AV	SonicWall	Application	N/A	1	1	Protection	Moderate	Moderate	3rd Party	3rd Party	JB Hong
2	SharePoint Server	Microsoft	Server	N/A	1.1		Protection,Processing	Moderate	Moderate	Company	Company	Scott Armstrong
3	Office 365 - GCC High	Microsoft	Cloud		2018		Processing	High	High	3rd Party	3rd Party	Azure Gov Cloud

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

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


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

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):

- 222 ✖
- assessment ✖
- auditor_list ✖
- https://my.exostar.com/download/attachments/43615568/Certification%20Assistant%20Standard%20Guide.pdf?version=1&modificationDate=1590589379733&api=v2 ✖

Narrative:

The System Description Document (SDD) is a top level informal document that describes what the system will do. It should describe the "System" or "Product" from a users' perspective. This is the first document that any auditor or contractor would read. From it they should understand what the system does.

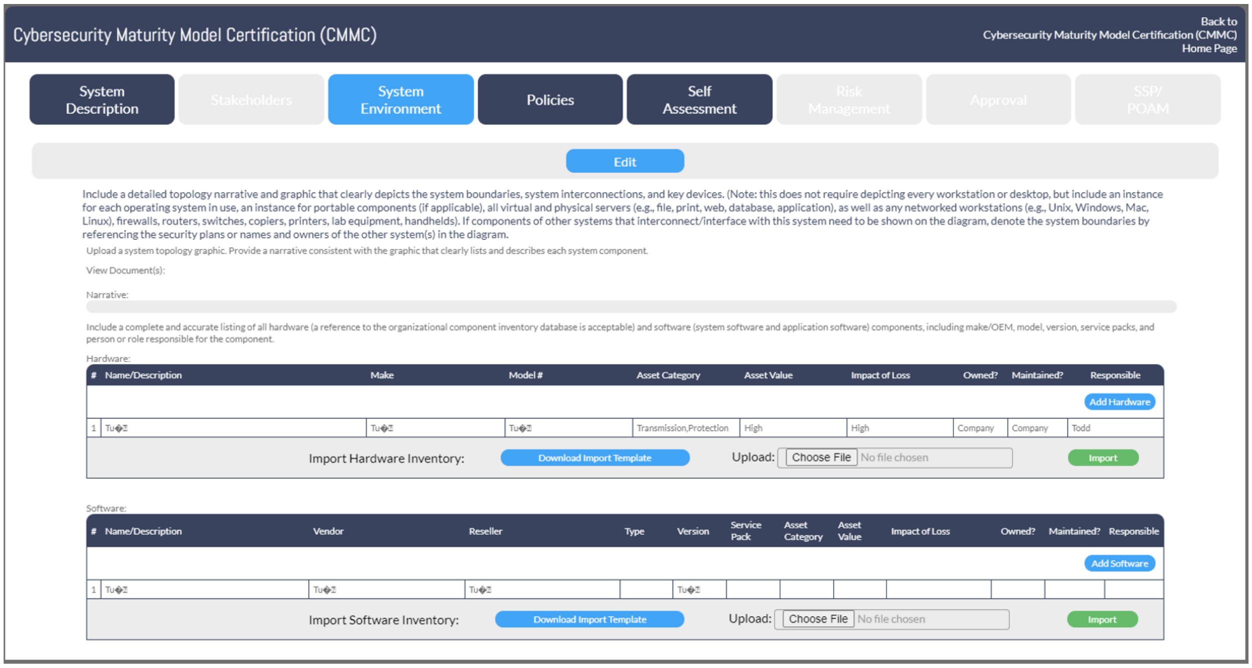
Include a complete and accurate listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Hardware:

#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
				□ Transmission □ Protection □ Processing	○ High ○ Moderate ○ Low	○ High ○ Moderate ○ Low	○ By Company ○ By 3rd Party	○ By Company ○ By 3rd Party	
						Save	Save & Add	Delete	Cancel
1	Router	Cisco	ASR 4000	Processing	Moderate	Moderate	Company	3rd Party	JB HONG
2	Storage	Sans Digital	XN3004T	Processing	High	High	Company	Company	JB Hong
3	Firewall	Cisco	FP42000	Protection,Processing	High	Moderate	Company	3rd Party	Trustwave
4	HP Server	HP	8888-DE	Transmission,Protection,Processing	Moderate	Moderate	3rd Party	3rd Party	JB Hong
5	Windows Laptop	Microsoft	xxxx	Transmission,Protection,Processing	Moderate	Moderate	Company	Company	JB Hong
6	Windows Laptop	Dell	AS1111	Transmission	Moderate	High	Company		JB Hong

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

You also can now upload your Hardware Inventory. The template needed is on the bottom of table. 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 Maturity Model Certification (CMMC)

Back to
Cybersecurity Maturity Model Certification (CMMC)
Home Page

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.

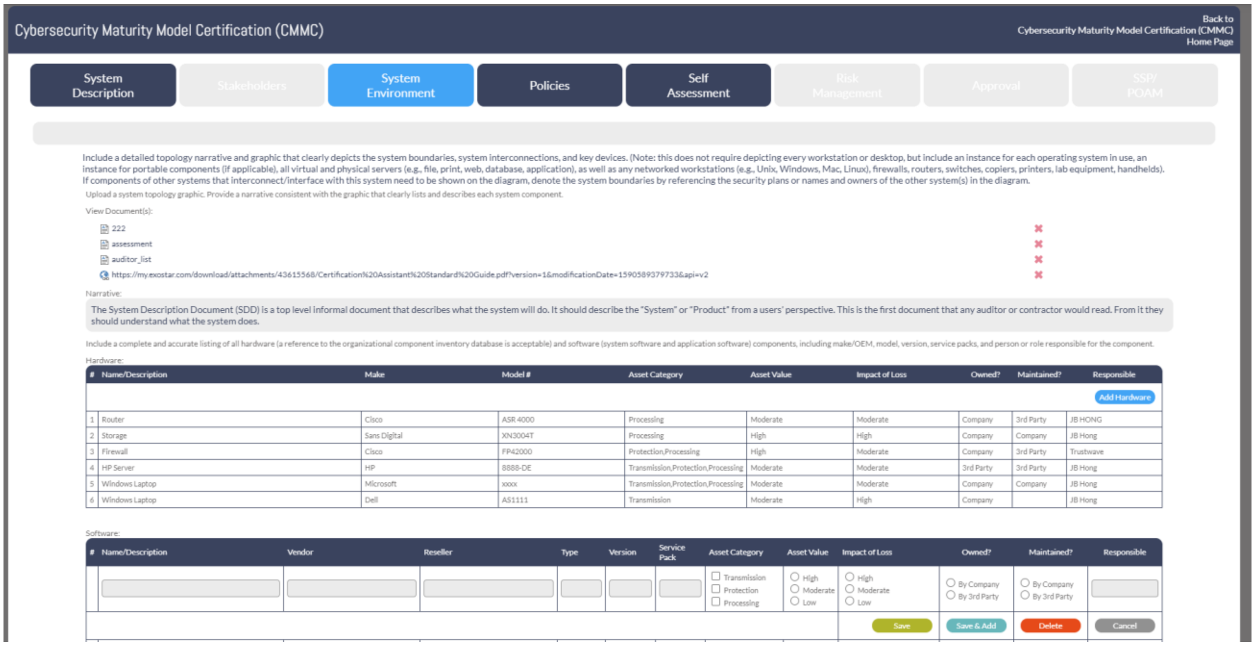
Hardware:

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

Software:

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

Software Inventory:



Cybersecurity Maturity Model Certification (CMMC)

Back to
Cybersecurity Maturity Model Certification (CMMC)
Home Page

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):

- 222 ✖
- assessment ✖
- auditor_list ✖
- https://my.exostar.com/download/attachments/43615568/Certification%20Assistant%20Standard%20Guide.pdf?version=1&modificationDate=1590589379733&api=v2 ✖

Narrative:

The System Description Document (SDD) is a top level informal document that describes what the system will do. It should describe the "System" or "Product" from a users' perspective. This is the first document that any auditor or contractor would read. From it they should understand what the system does.

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	Router	Cisco	ASR 4000	Processing	Moderate	Moderate	Company	3rd Party	JB HONG
2	Storage	Sans Digital	XN3004T	Processing	High	High	Company	Company	JB Hong
3	Firewall	Cisco	FP42000	Protection,Processing	High	Moderate	Company	3rd Party	Trustwave
4	HP Server	HP	8888-DE	Transmission,Protection,Processing	Moderate	Moderate	3rd Party	3rd Party	JB Hong
5	Windows Laptop	Microsoft	xxxx	Transmission,Protection,Processing	Moderate	Moderate	Company	Company	JB Hong
6	Windows Laptop	Dell	AS1111	Transmission	Moderate	High	Company		JB Hong

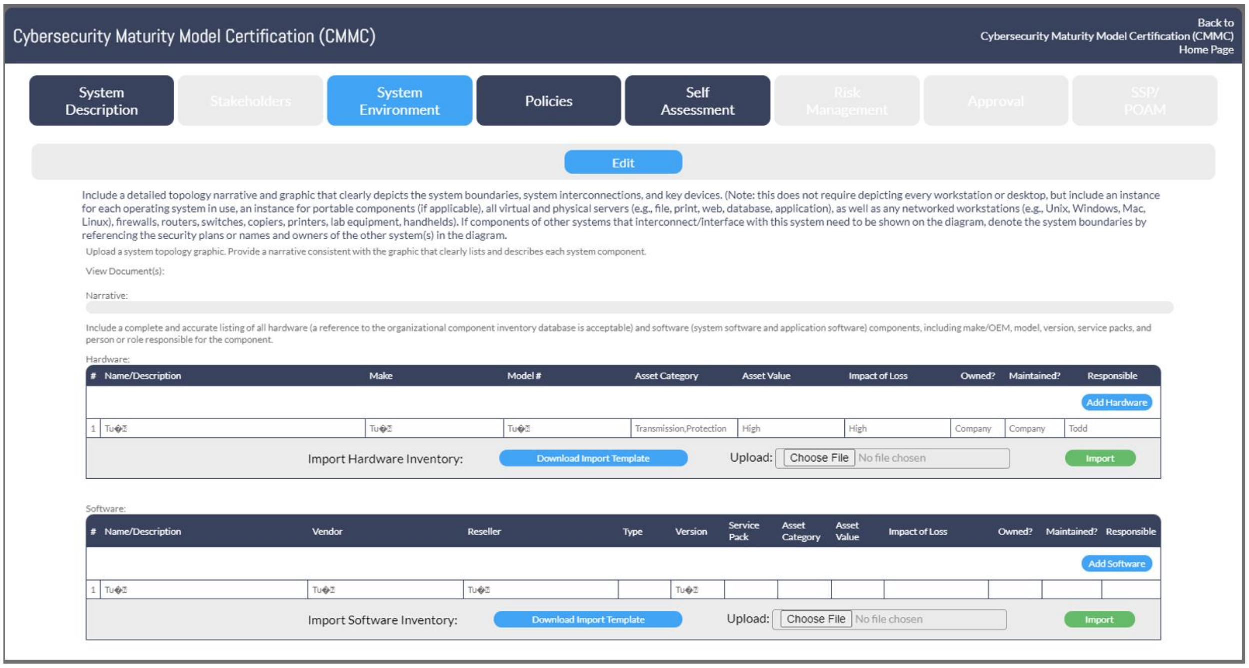
Software:

#	Name/Description	Vendor	Reseller	Type	Version	Service Pack	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
							□ Transmission □ Protection □ Processing	○ High ○ Moderate ○ Low	○ High ○ Moderate ○ Low	○ By Company ○ By 3rd Party	○ By Company ○ By 3rd Party	

To list your Software Inventory, use the Add Software button. This will open the form to add software to the list. The following fields will need to be entered: Name/Description, Vendor, Reseller, Type, Version, Service Pack, Responsible, and then select from the options for Asset

Category, Asset Value, Impact of Loss (related to Risk Management), Owned, and Maintained for the software.

You also can now upload your Software Inventory. The template needed is on the bottom of table. 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 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

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:

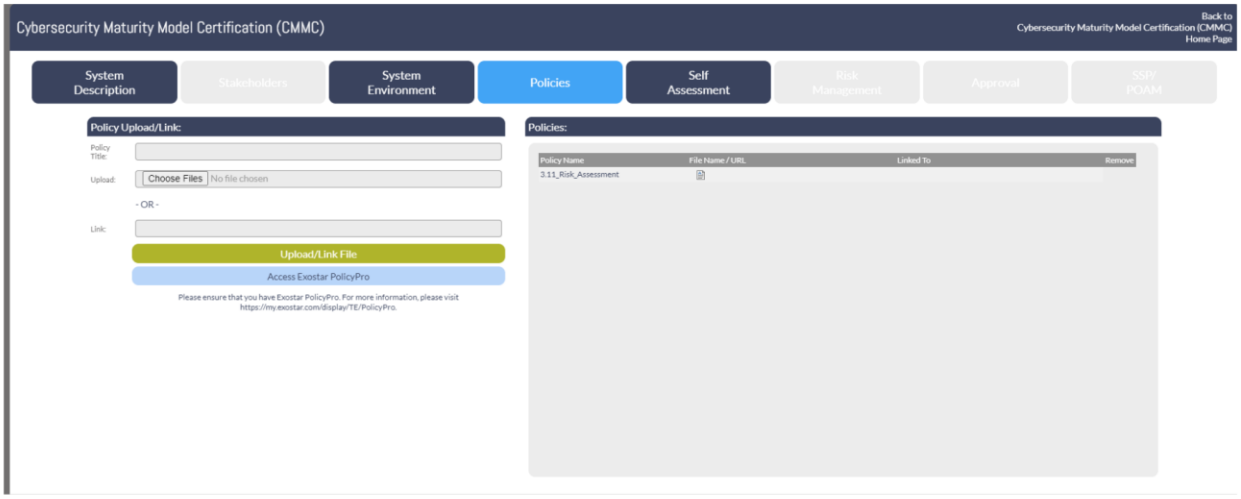
#	Name/Description	Make	Model #	Asset Category	Asset Value	Impact of Loss	Owned?	Maintained?	Responsible
1	Tu�Σ	Tu�Σ	Tu�Σ	Transmission,Protection	High	High	Company	Company	Todd

Software:

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

Policies Tab

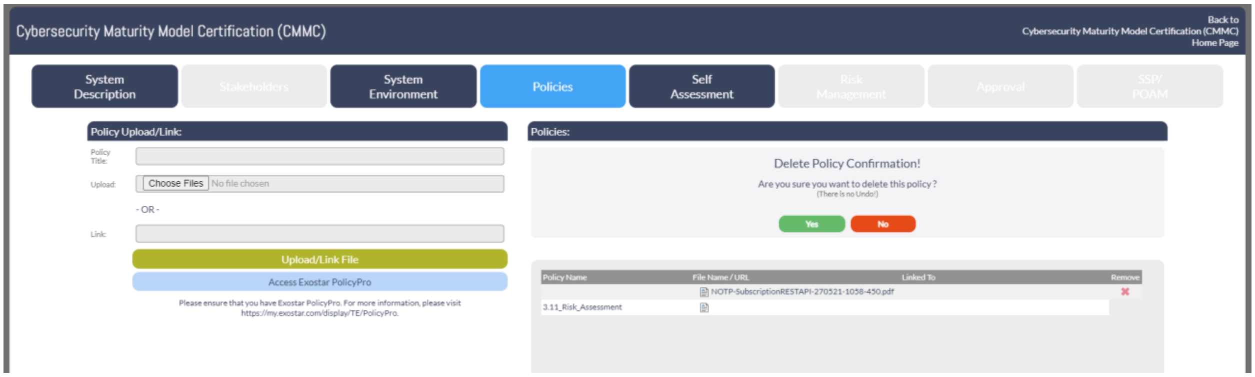
The Policies tab is used as a repository for all policy documentation referred to in the controls. Click on the button to choose your files – multiple files can be uploaded at the same time. You can add the link to Certification Assistant for files that are stored and available externally. Use the blue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



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

Policy Name	File Name / URL	Linked To	Remove
3.11_Risk_Assessment	🗎		

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



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

Delete Policy Confirmation!

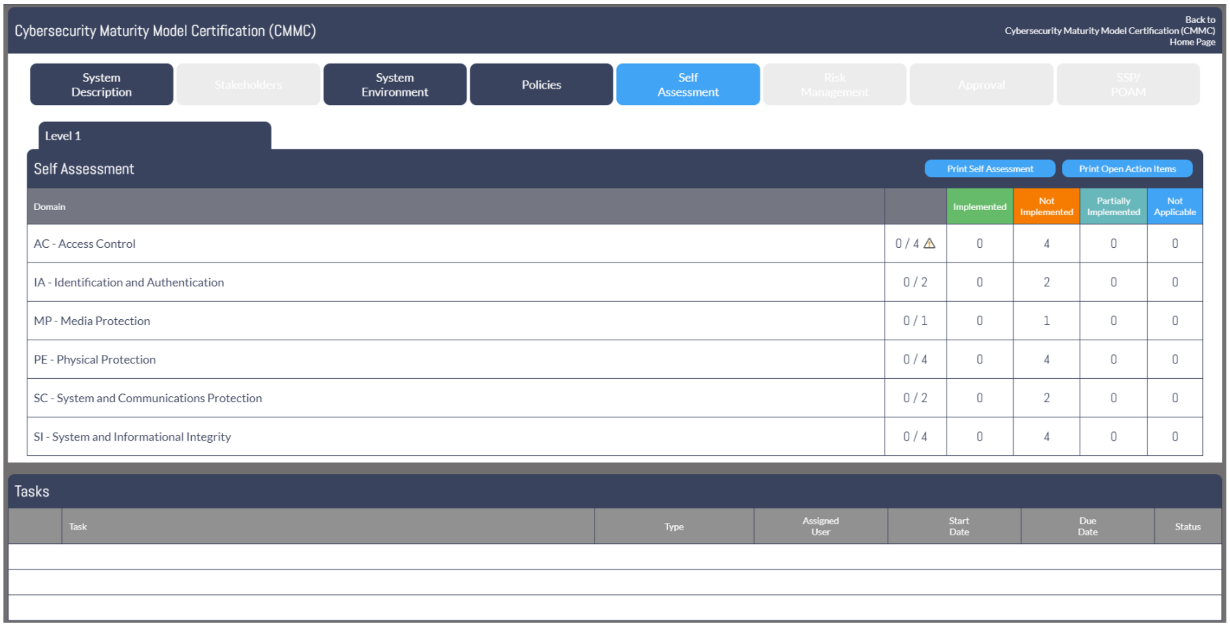
Are you sure you want to delete this policy ?
(There is no Undo!)

Policy Name	File Name / URL	Linked To	Remove
	🗎 NOTP-SubscriptionRESTAPI-270521-1058-450.pdf		✖
3.11_Risk_Assessment	🗎		

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

Self-Assessment Tab

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



Cybersecurity Maturity Model Certification (CMMC)

Self Assessment

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

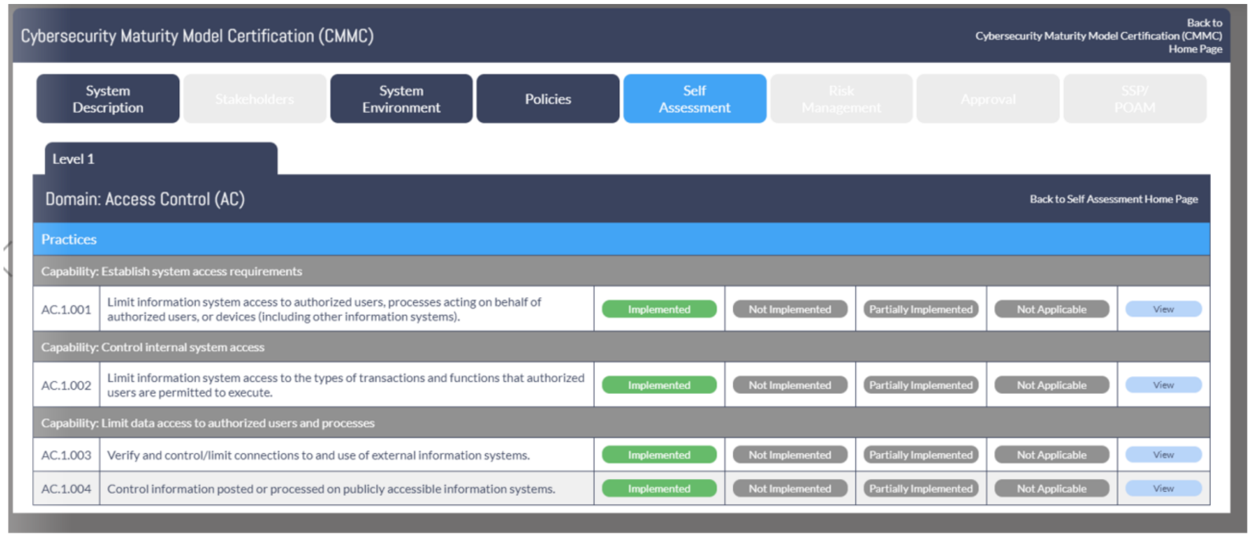
Tasks

	Task	Type	Assigned User	Start Date	Due Date	Status

The upper section is a list of the Domains available in the Level, the lower section is all open Action Items for the CMMC program.

Click on a Domain name (Access Control in this instance) and the Practices within that domain are displayed. Click on the View button or click on the practice content to view the control details.

You can now decision any individual control from the Domain Dashboard page. Please note that you still need to add implementation statements and add documentation to inform that status … this can just help facilitate a run thru of the controls.



Cybersecurity Maturity Model Certification (CMMC)

Back to Cybersecurity Maturity Model Certification (CMMC) Home Page

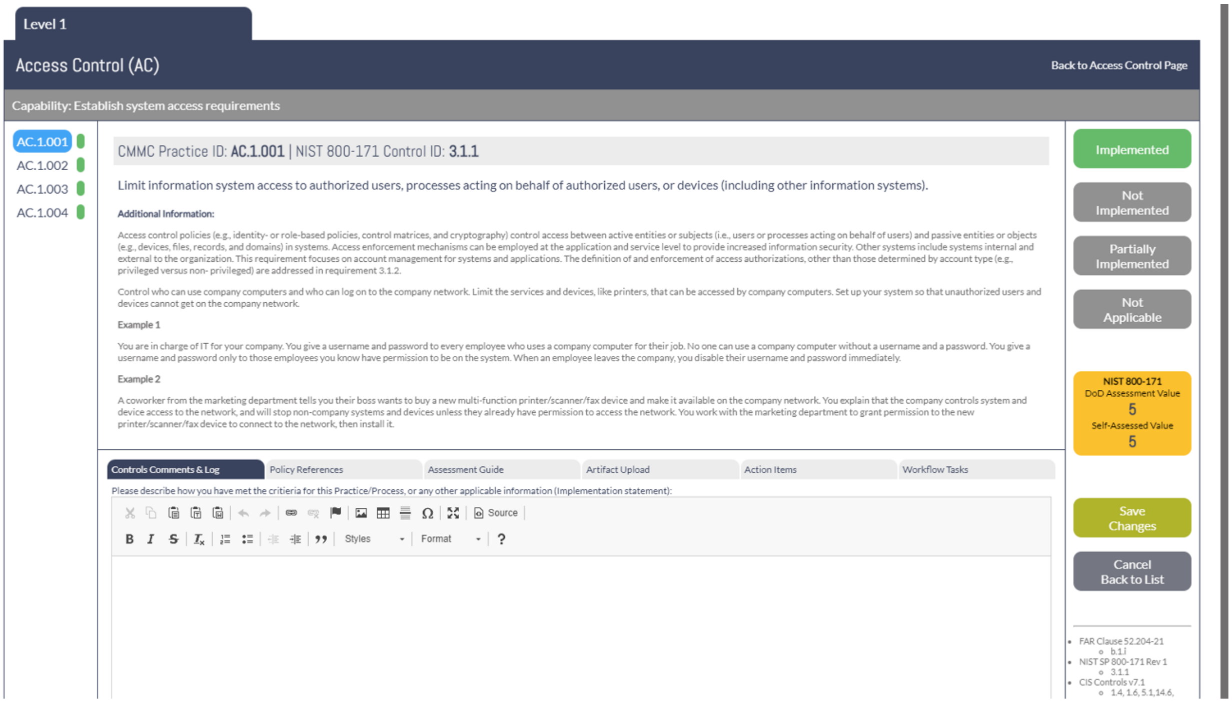
Level 1

Domain: Access Control (AC)

Back to Self Assessment Home Page

Practices

Capability: Establish system access requirements						
AC.1.001	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
Capability: Control internal system access						
AC.1.002	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
Capability: Limit data access to authorized users and processes						
AC.1.003	Verify and control/limit connections to and use of external information systems.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View
AC.1.004	Control information posted or processed on publicly accessible information systems.	Implemented	Not Implemented	Partially Implemented	Not Applicable	View



Level 1

Access Control (AC)

Back to Access Control Page

Capability: Establish system access requirements

CMMC Practice ID: **AC.1.001** | NIST 800-171 Control ID: **3.1.1**

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Additional Information:

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 non- privileged) are addressed in requirement 3.1.2.

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

A coworker from the marketing department tells you their boss wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

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

NIST 800-171
DoD Assessment Value
5
Self-Assessed Value
5

- FAR Clause 52.204-21
  - b.1.i
- NIST SP 800-171 Rev 1
  - 3.1.1
- CIS Controls v7.1
  - 1.4, 1.6, 5.1,14.6,

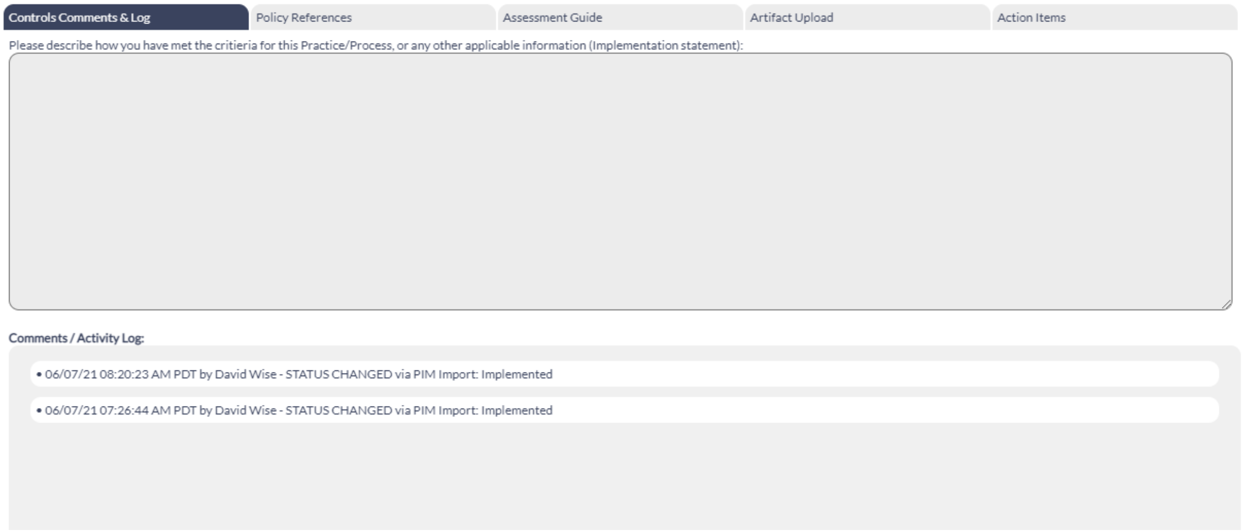
The Control Detail page has 3 main components

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



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

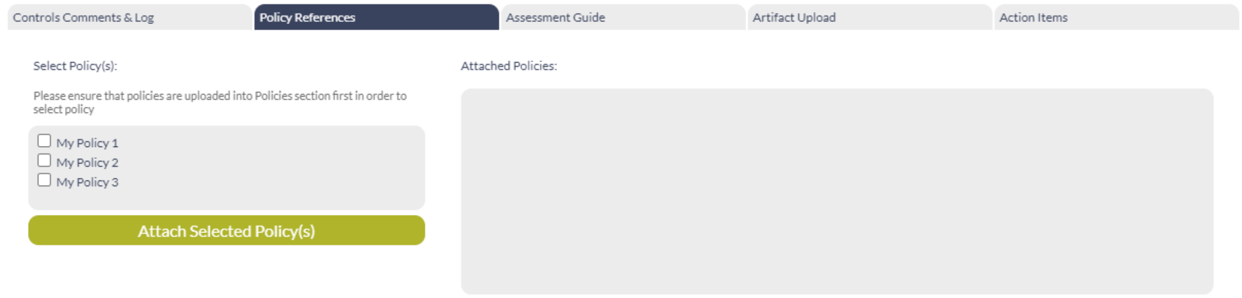
Comments / Activity Log:

- 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 for 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



Select Policy(s):

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

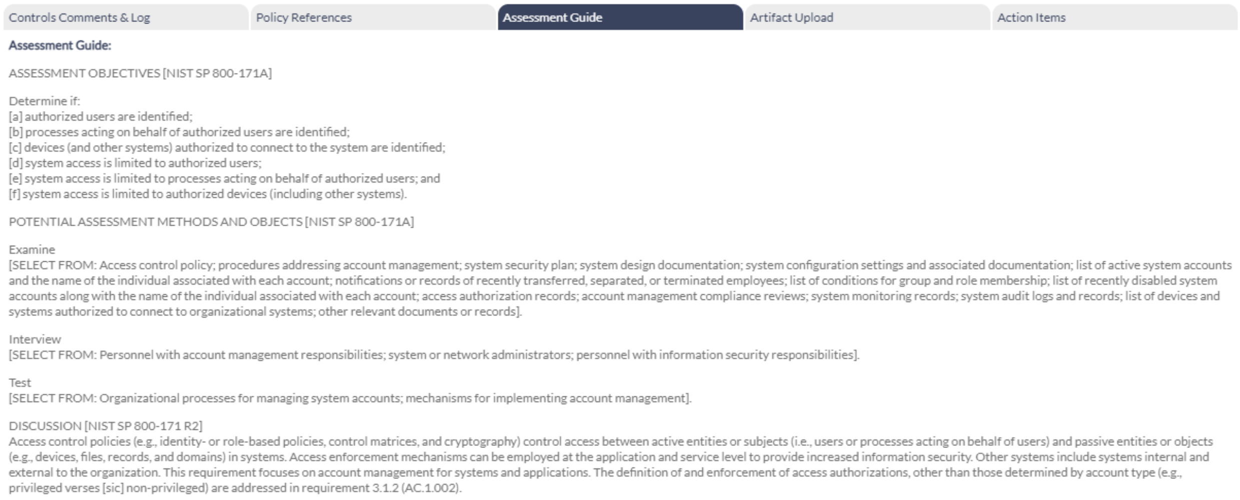
□ My Policy 1
□ My Policy 2
□ My Policy 3

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



Assessment Guide:

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

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

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

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

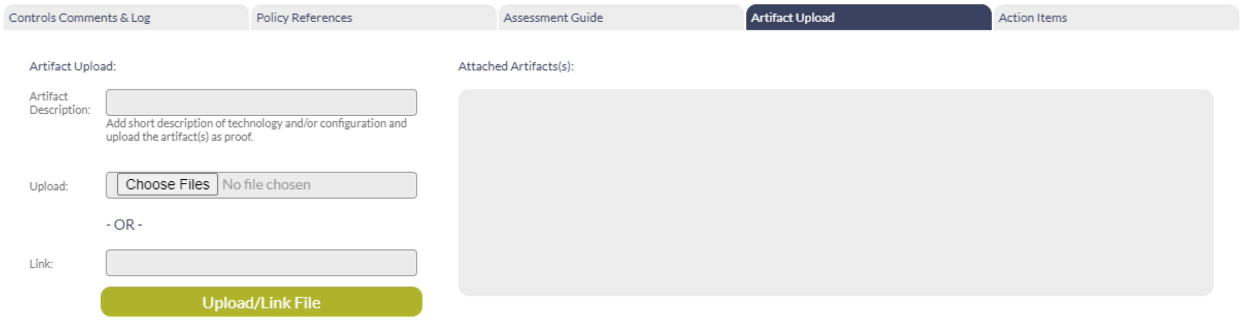
Interview
[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

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

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

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

Tab 4 – Artifact Upload



Artifact Description:

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

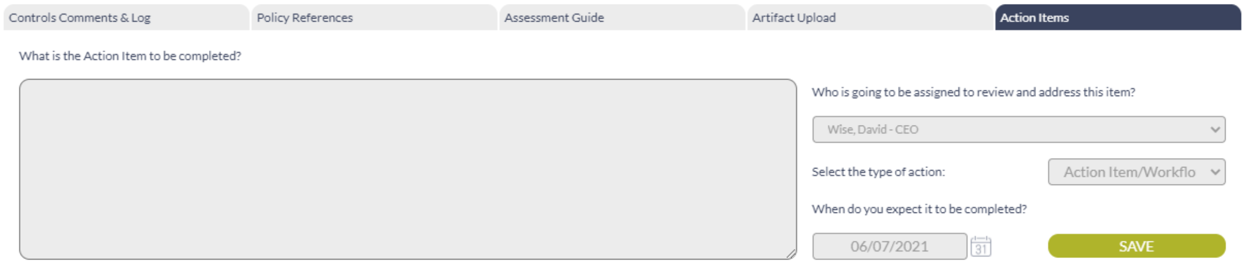
Upload: No file chosen

Link:

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



What is the Action Item to be completed?

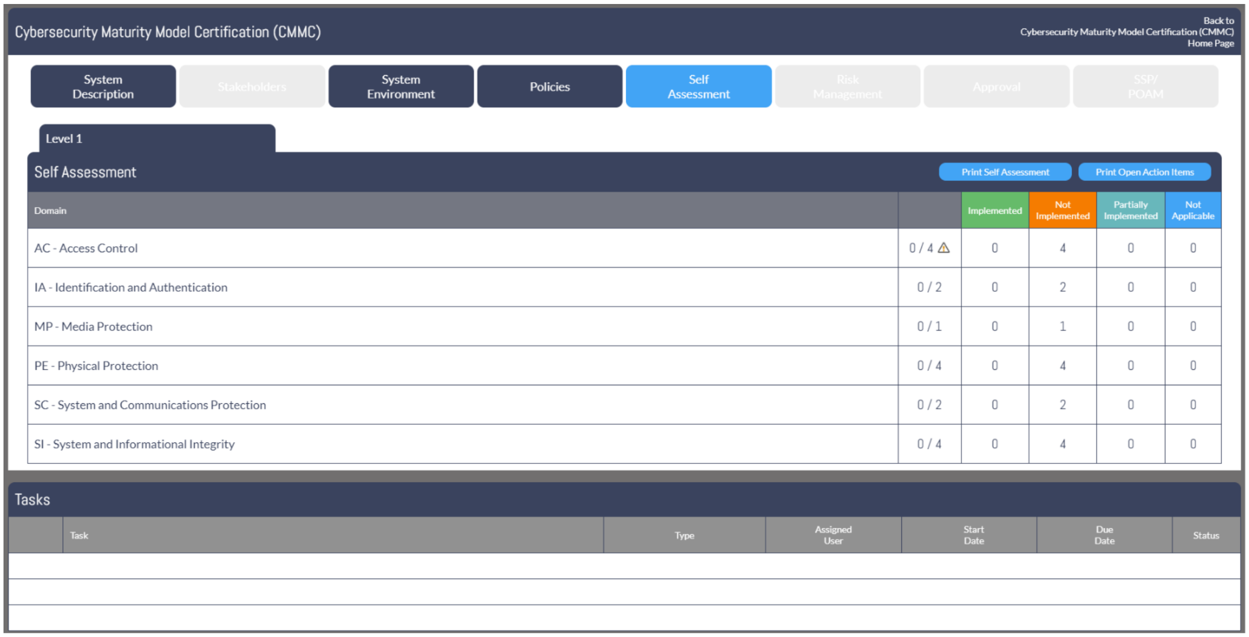
Who is going to be assigned to review and address this item? Wise, David - CEO

Select the type of action: Action Item/Workflo

When do you expect it to be completed? 06/07/2021

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 an Action Item/Workflow, 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.

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.

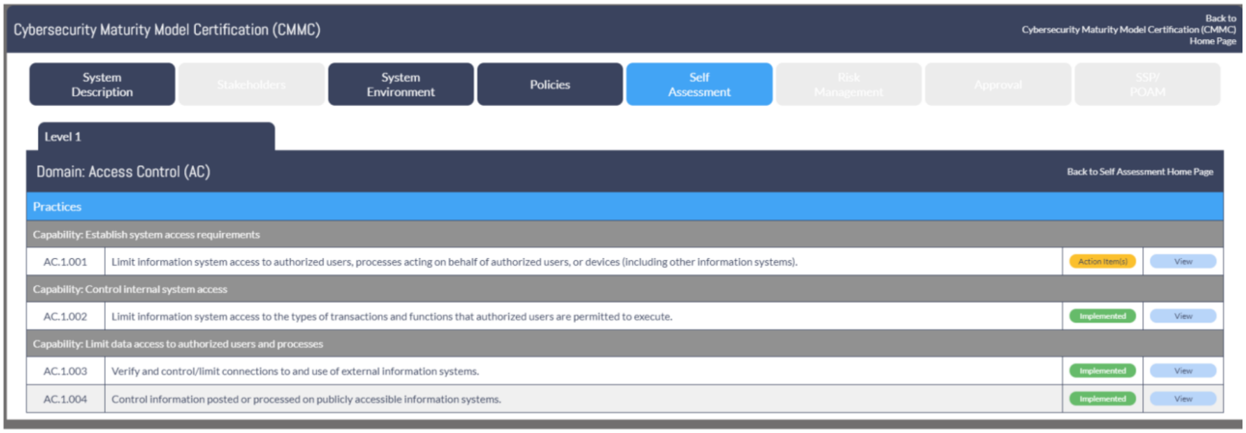


Self Assessment

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

Tasks

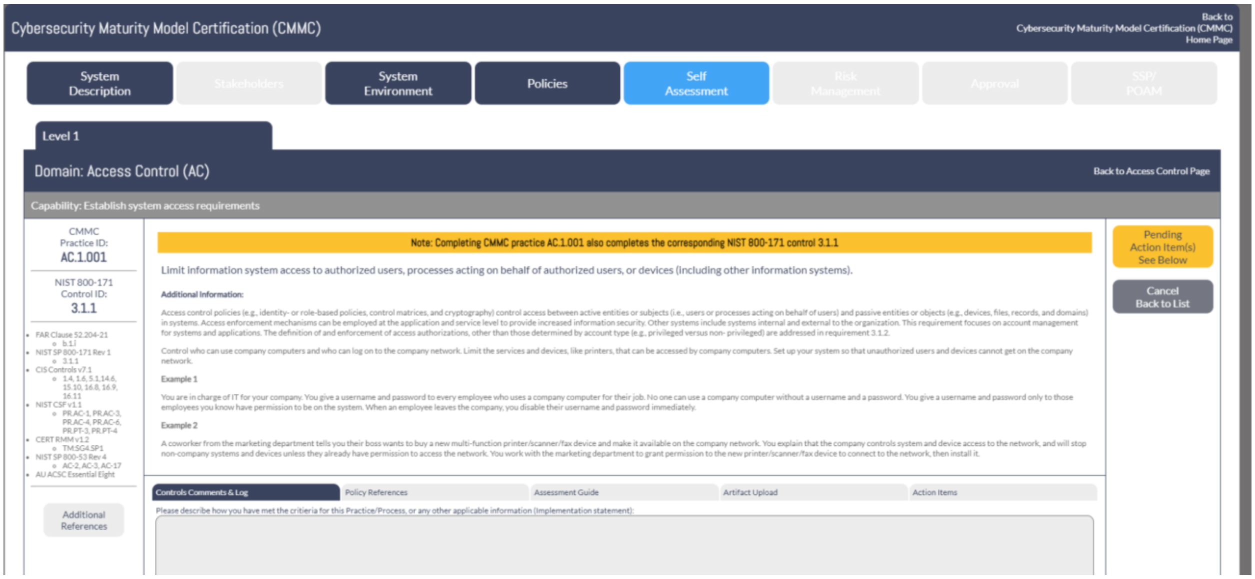
	Task	Type	Assigned User	Start Date	Due Date	Status


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
Level 1
Back to Self Assessment Home Page

Domain: Access Control (AC)

Practices

Capability: Establish system access requirements			
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Action Item(s)	View
Capability: Control internal system access			
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Implemented	View
Capability: Limit data access to authorized users and processes			
AC.1.003	Verify and control/limit connections to and use of external information systems.	Implemented	View
AC.1.004	Control information posted or processed on publicly accessible information systems.	Implemented	View



Domain: Access Control (AC)

Capability: Establish system access requirements

CMMC Practice ID: AC.1.001

NIST 800-171 Control ID: 3.1.1

- FAR Clause 52.204-21
  - b.1.i
- NIST SP 800-171 Rev 1
  - 3.1.1
- CIS Controls v7.1
  - 1.4, 1.6, 5.1,14.6, 15.10, 16.8, 16.9, 16.11
- NIST CSF v1.1
  - PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
- CERT RMM v1.2
  - TM:SG4.SP1
- NIST SP 800-53 Rev 4
  - AC-2, AC-3, AC-17
- AU ACSC Essential Eight

Note: Completing CMMC practice AC.1.001 also completes the corresponding NIST 800-171 control 3.1.1

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Additional Information:

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 non- privileged) are addressed in requirement 3.1.2.

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

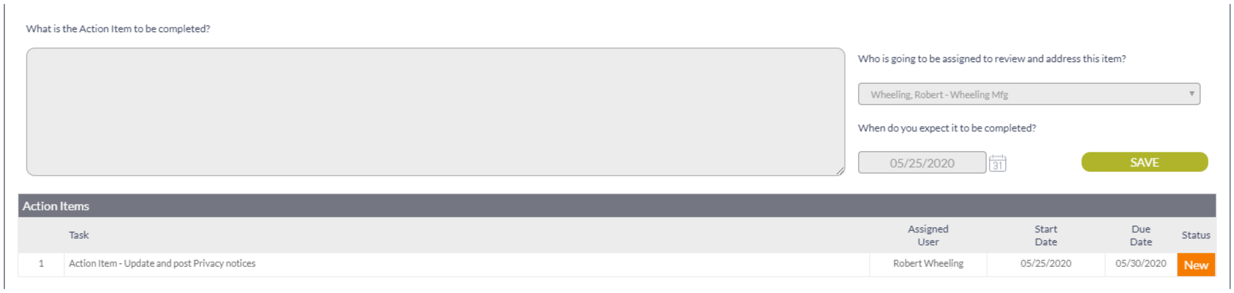
You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

A coworker from the marketing department tells you their boss wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

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

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

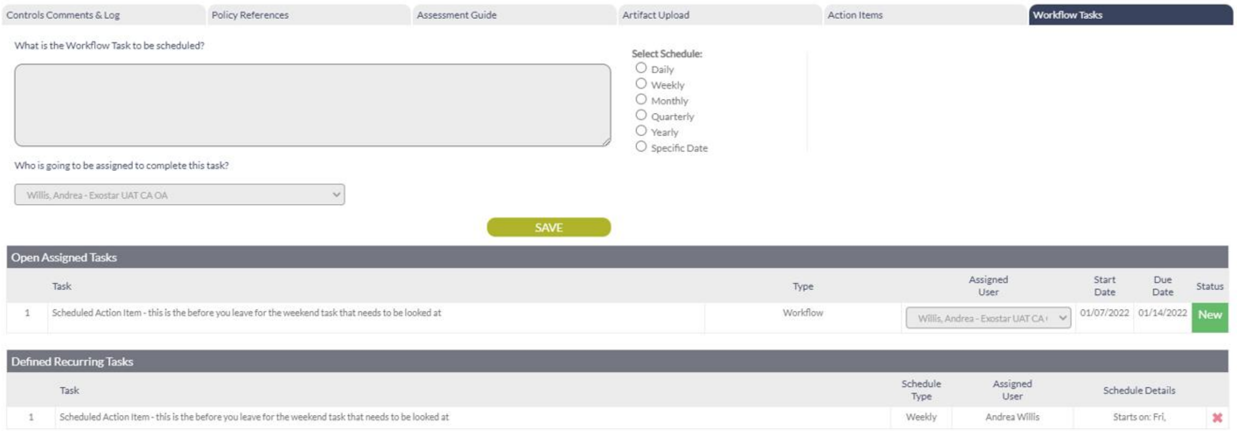
When do you expect it to be completed?

05/25/2020

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

Tab 6 – Workflow Tasks



What is the Workflow Task to be scheduled?

Select Schedule:
○ Daily
○ Weekly
○ Monthly
○ Quarterly
○ Yearly
○ Specific Date

Who is going to be assigned to complete this task?

Willis, Andrea - Exostar UAT CA OA

Open Assigned Tasks

	Task	Type	Assigned User	Start Date	Due Date	Status
1	Scheduled Action Item - this is the before you leave for the weekend task that needs to be looked at	Workflow	Willis, Andrea - Exostar UAT CA	01/07/2022	01/14/2022	New

Defined Recurring Tasks

	Task	Schedule Type	Assigned User	Schedule Details	
1	Scheduled Action Item - this is the before you leave for the weekend task that needs to be looked at	Weekly	Andrea Willis	Starts on: Fri,	✖

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

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

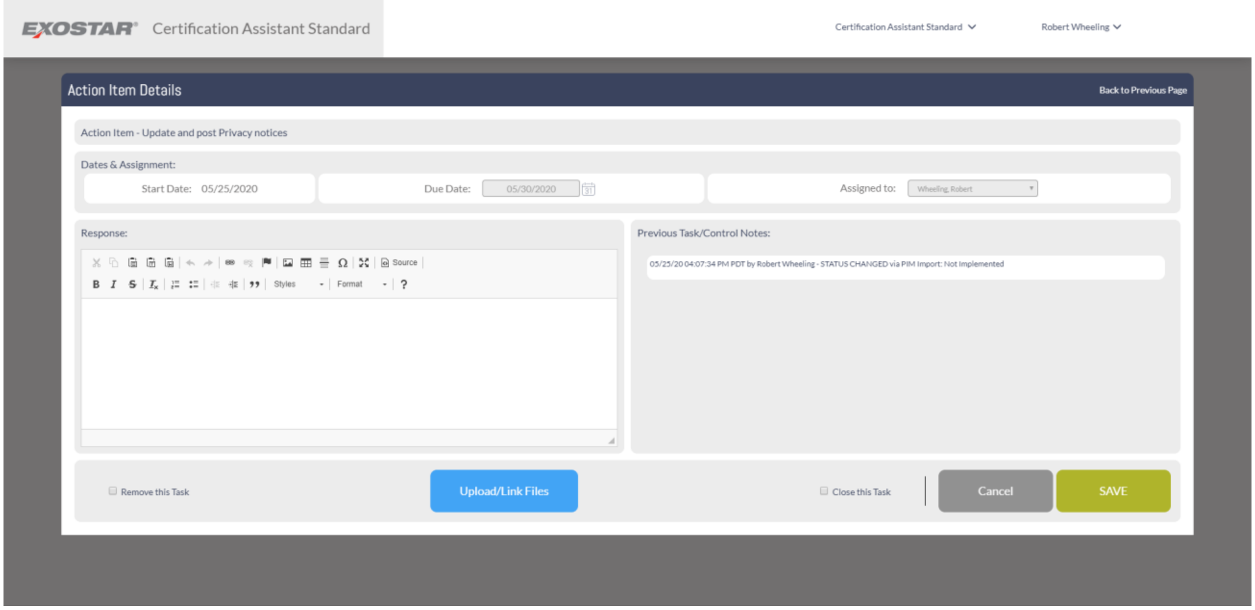
Once a task has been created you will see it in the bottom section, Defined Recurring Tasks. If no longer needed, the task can be removed by clicking the X.

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

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

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.



Action Item Details

Action Item - Update and post Privacy notices

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 PDT by Robert Wheeling - STATUS CHANGED via PIM Import: Not Implemented

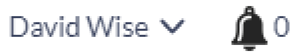
□ Remove this Task

□ Close this Task

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

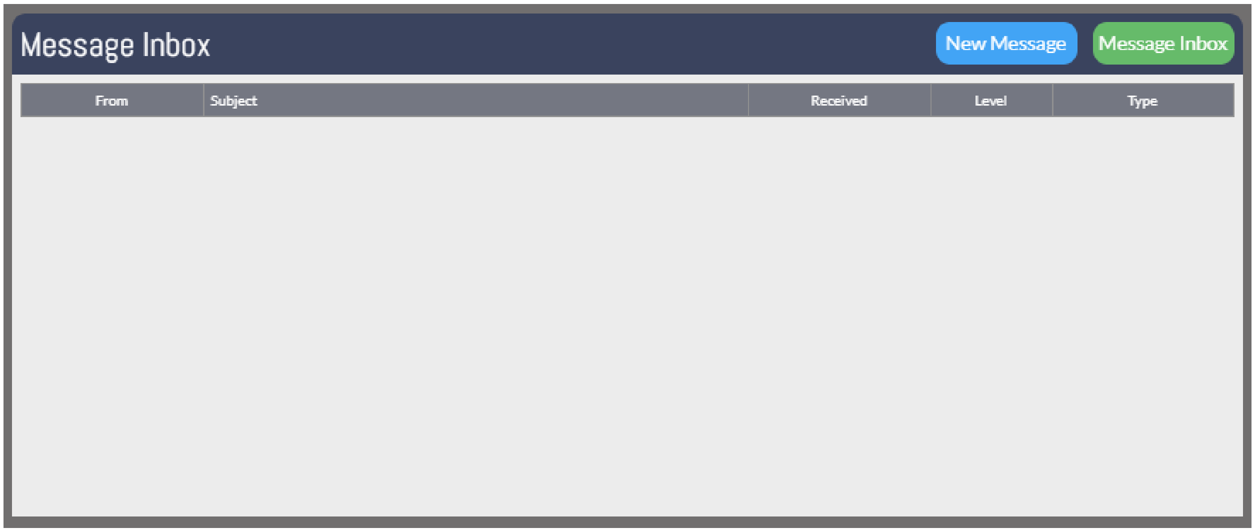
Certification Assistant Messaging

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

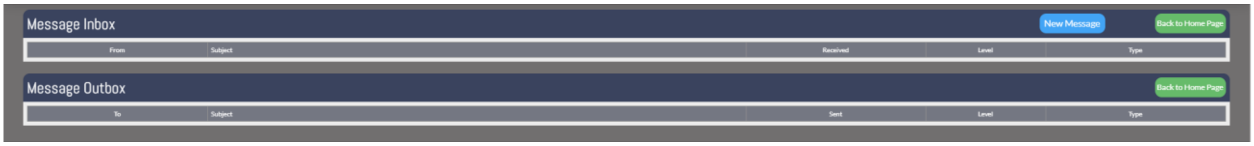


If the number next to the bell is higher than 0, then you have new messages waiting.

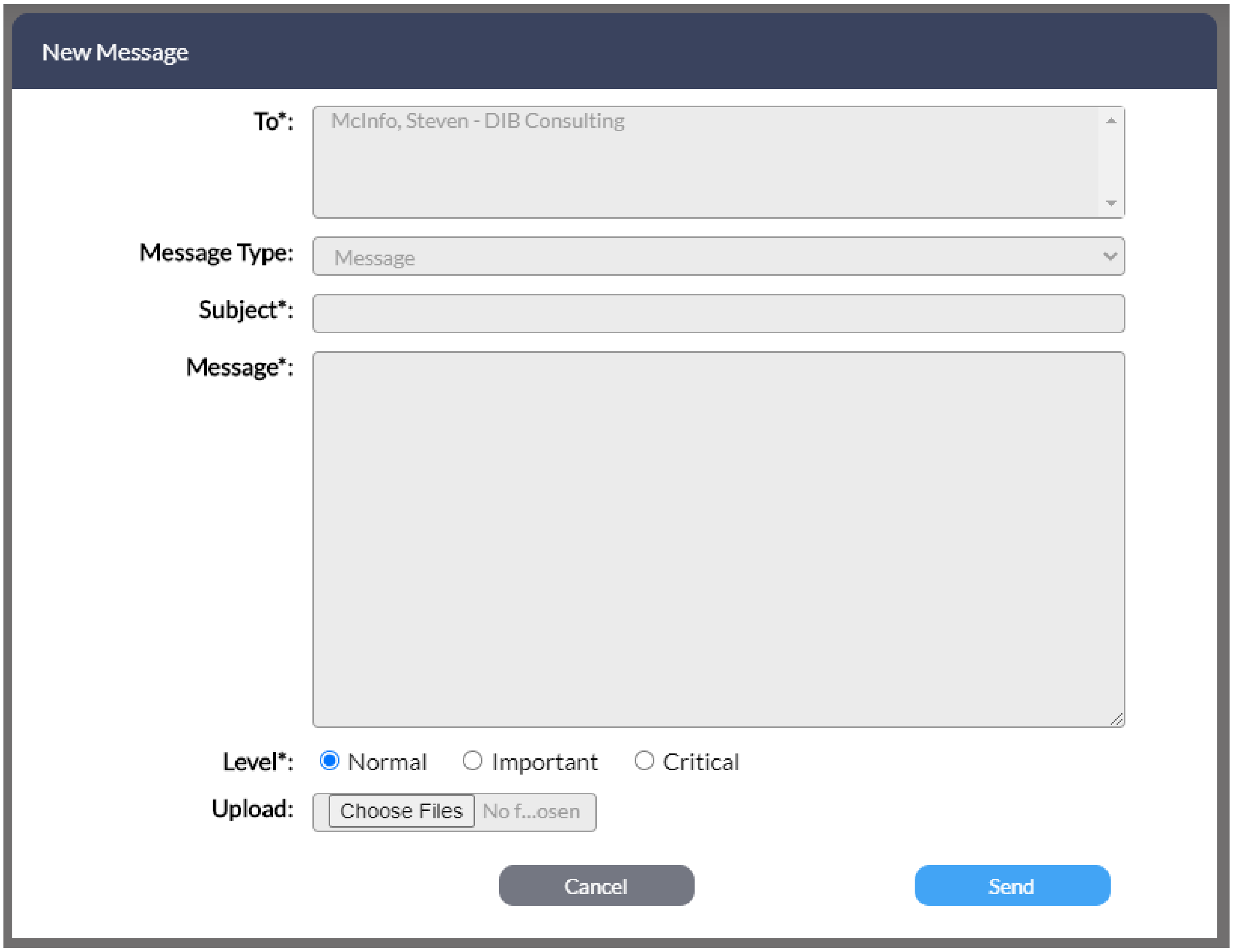
Your messages will appear in the Message Inbox on the homepage.



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.



New Message

To*: McInfo, Steven - DIB Consulting

Message Type: Message

Subject*:

Message*:

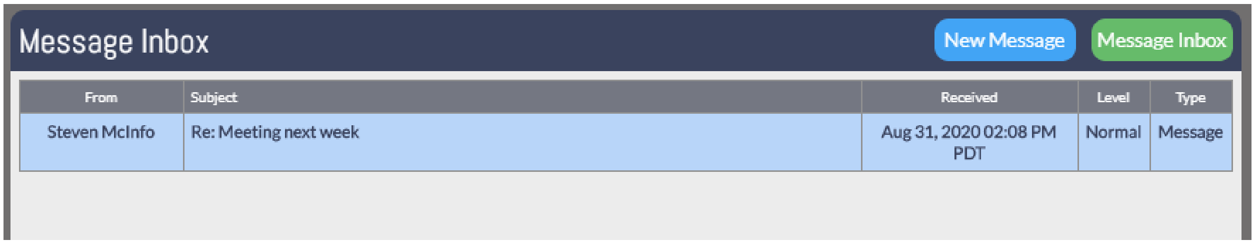
Level*: ● Normal ○ Important ○ Critical

Upload: Choose Files No f...osen

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.

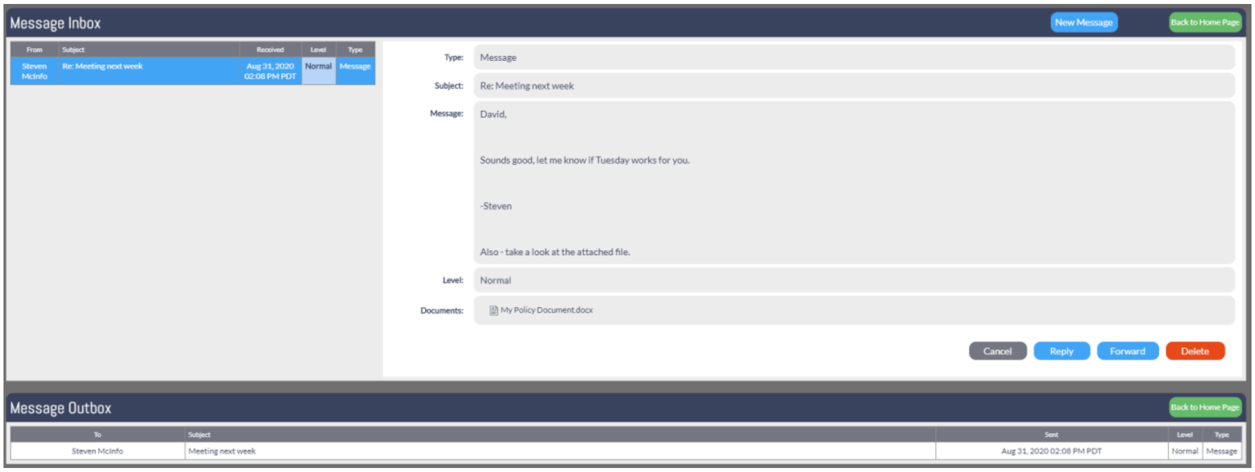
Select your Message Type, enter a subject and enter your message. Select the Level for the message and attach files if needed. Any files attached will be uploaded and encrypted. Click the Send button and the message will show up in your sent list.

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



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.



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

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

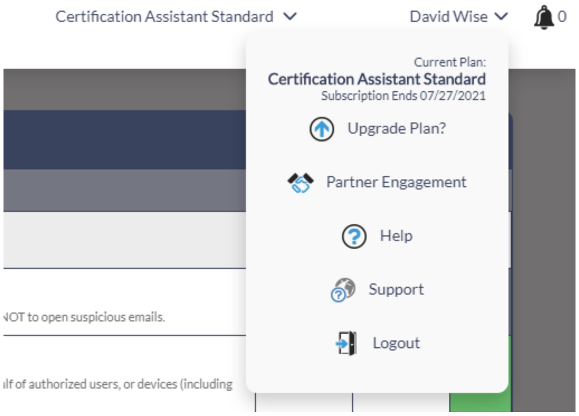
Documents: My Policy Document.docx

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.

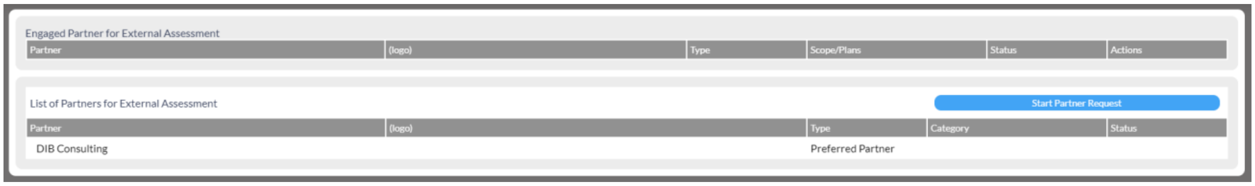
Partner Engagement

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.


Certification Assistant Standard
David Wise
0
Upgrade Plan?
Partner Engagement
Help
Support
Logout
NOT to open suspicious emails.
alf of authorized users, or devices (including

Current Plan:
Certification Assistant Standard
Subscription Ends 07/27/2021

To begin, click on the Start Partner Request button.



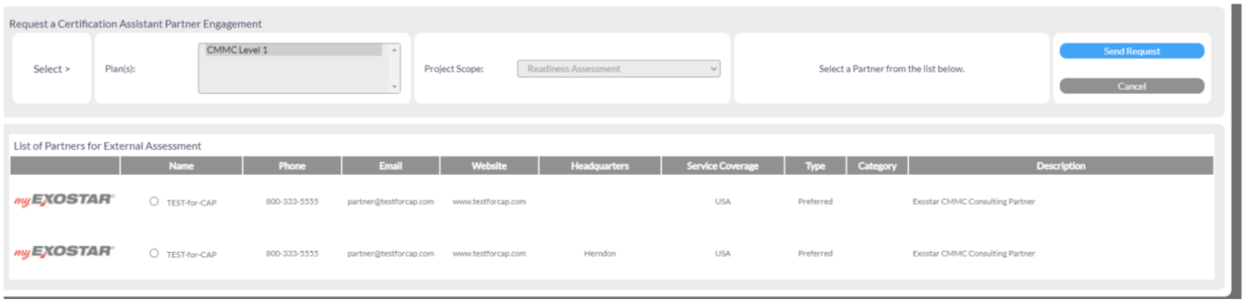
Engaged Partner for External Assessment

Partner	(logo)	Type	Scope/Plans	Status	Actions

List of Partners for External Assessment

Start Partner Request

Partner	(logo)	Type	Category	Status
DIB Consulting		Preferred Partner		



Request a Certification Assistant Partner Engagement

Select > Plan(s): CMMC Level 1

Project Scope: Readiness Assessment

Select a Partner from the list below.

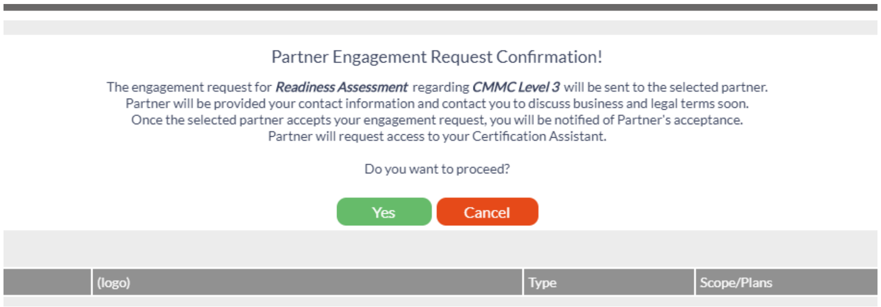
Send Request

Cancel

List of Partners for External Assessment

	Name	Phone	Email	Website	Headquarters	Service Coverage	Type	Category	Description
myEXOSTAR	○ TEST-for-CAP	800-333-5555	partner@testforcap.com	www.testforcap.com		USA	Preferred		Exostar CMMC Consulting Partner
myEXOSTAR	○ TEST-for-CAP	800-333-5555	partner@testforcap.com	www.testforcap.com	Herndon	USA	Preferred		Exostar CMMC Consulting Partner

Select the Plan(s) to be assessed, CMMC Level 1. 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?

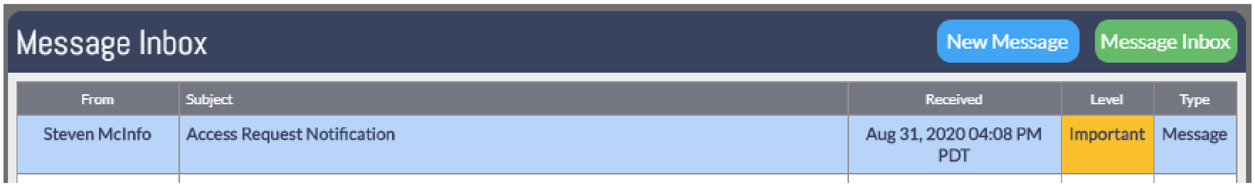
Yes Cancel

	(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.

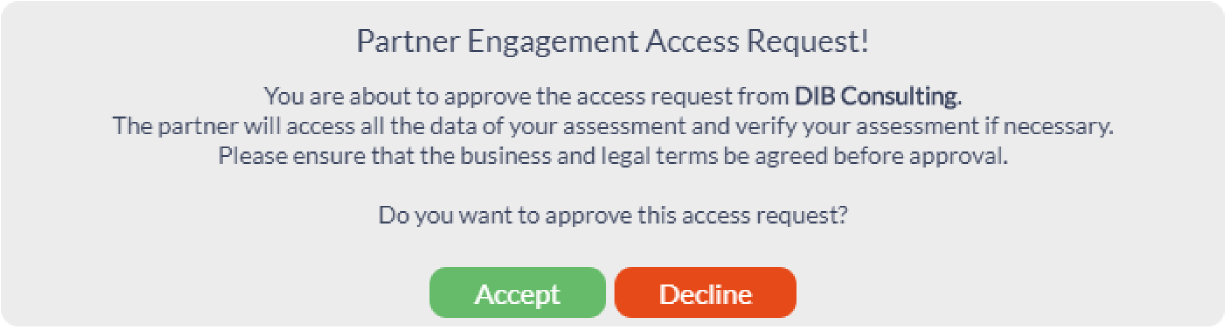
Once accepted, the status will update to Engagement Accepted. The partner will then assign a consultant to your engagement and they will request access to your data in Certification Assistant. You will receive a message from the system that this request has been sent.



Message Inbox

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.



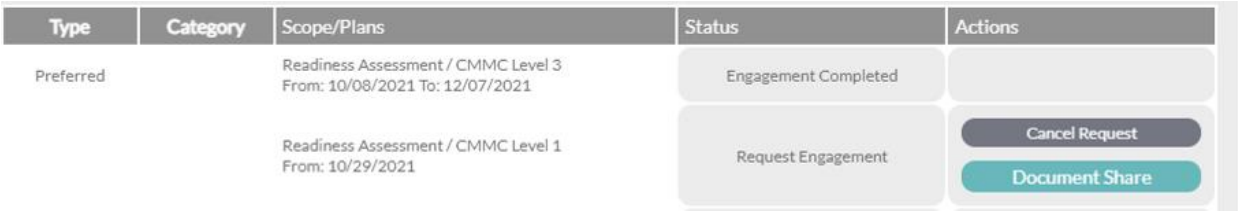
Partner Engagement Access Request!

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?

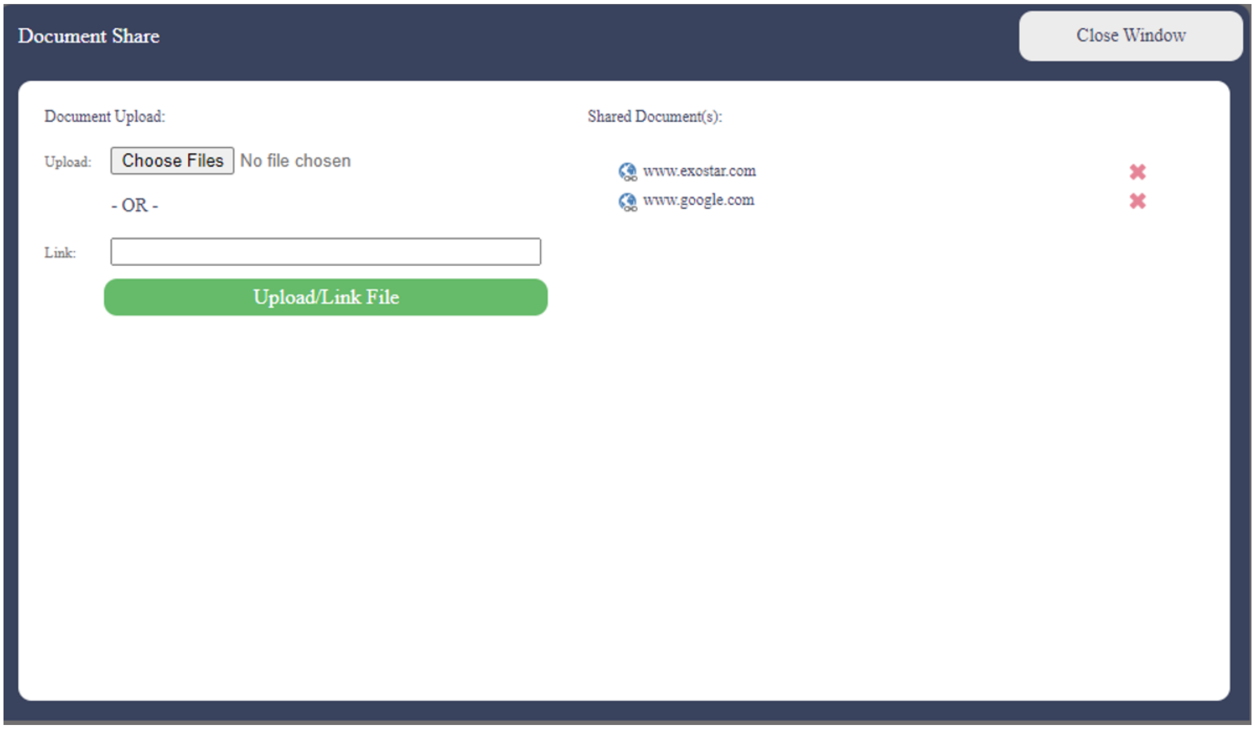
If you choose to accept, the consultant will be able to access your data from their login and review, make comments, assign actions, and upload documentation just like a member of your account. When they have completed their work, they will cancel access and move on to the documentation stage of the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

At any time during an engagement, you and the partner now have the ability to share documents.



Type	Category	Scope/Plans	Status	Actions
Preferred		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

Clicking on Document Share will open a pop-up window to load either a document(s) or link(s).



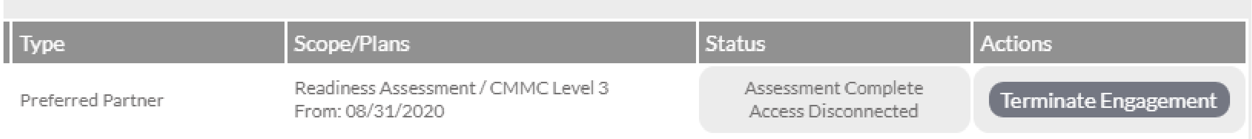
No file chosen

www.exostar.com ✖

www.google.com ✖

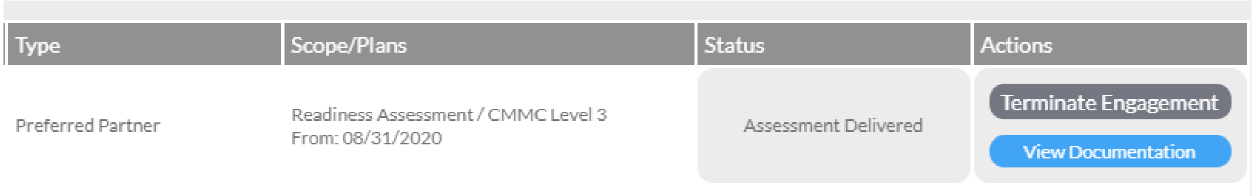
NOTE: Once the engagement is terminated, access to these documents is removed.

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



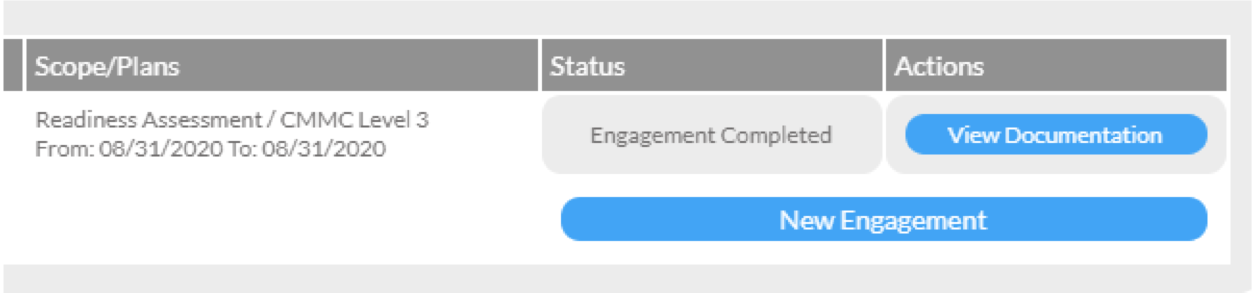
Type	Scope/Plans	Status	Actions
Preferred Partner	Readiness Assessment / CMMC Level 3 From: 08/31/2020	Assessment Complete Access Disconnected	Terminate Engagement

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