



COMPLIANCE MANAGERTM

by RapidFireTools[®]

QUICK START GUIDE

Compliance Manager for CMMC (Cybersecurity
Maturity Model Certification)

Instructions to Perform a CMMC Assessment

Contents

Performing a CMMC Assessment	4
<u>Compliance Manager for CMMC</u>	4
<u>Compliance Manager for CMMC Assessment Overview</u>	5
Network Prerequisites for Assessment Scans	6
<u>Pre-Scan Network Configuration Checklist</u>	7
Checklist for Domain Environments	7
Checklist for Workgroup Environments	9
<u>Step 1 — Add Organizations</u>	12
Add an Organization	12
<u>Step 2 — Create a New Site</u>	15
<u>Step 3 — Use the To Do List to Complete Tasks</u>	22
Re-run or Modify To Do Items	22
Assessment Progress Bar	24
<u>Step 4 — Set Up the CMMC Assessment Project</u>	26
<u>Step 5 — Install and Configure the Compliance Manager Server</u>	33
Configure Scan Settings for Active Directory Domain	34
Configure Scan Settings for Workgroup	42
<u>Step 6 — Start Assessment and Perform Pre-Scan Analysis</u>	49
<u>Step 7 — Collect CMMC Assessment Data</u>	53
Attach Supporting Documents	56
Select Multiple Fields	58
Copy and Paste Responses	59
Which CMMC Level Should I Choose?	66
Change Assessment Level	66
<u>Step 8A — Complete Level 1 CMMC Worksheets</u>	68
Note Regarding Worksheet Cross References to NIST SP 800-171	68
<u>Step 8B — Complete Level 2 CMMC Worksheets</u>	75
Note Regarding Worksheet Cross References to NIST SP 800-171	75

<u>Step 8C — Complete Level 3 CMMC Worksheets</u>	93
Note Regarding Worksheet Cross References to NIST SP 800-171	93
<u>Step 9 — Document Compensating Controls</u>	109
<u>Step 10 — Generate CMMC Assessment Reports</u>	111
Optional Task: Export Issues to Kaseya BMS	112
Step 1 — Gather Credentials and Set Up Kaseya BMS	112
Step 2 — Set Up a Connection to your Kaseya BMS	113
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS	118
Step 4 — Export Issues to Kaseya BMS	119
<u>Step 11 — Complete and Archive your CMMC Assessment</u>	121
Archiving Assessments	121
<u>Step 12 — Start a New CMMC after Completing a Previous Assessment</u>	122
CMMC Assessment Reports	123
CMMC Compliance Reports	123
Supporting Documentation	126
Worksheets by Assessment Level	127
CMMC Risk Update Assessment Reports	132
Appendices	133
Pre-Scan Network Configuration Checklist	134
Checklist for Domain Environments	134
Checklist for Workgroup Environments	136
CMMC To Do Task Complete List	139

Performing a CMMC Assessment

Compliance Manager for CMMC

The **Cybersecurity Maturity Model Certification** (CMMC) presents a standard for achieving cybersecurity for companies that comprise the defense industrial base (DIB). The United States Department of Defense (DoD) formulated the CMMC to improve the cyber-security posture of the DIB supply-chain.

Compliance Manager for CMMC combines automated data collection with a structured framework for collecting supplemental assessment information not available through automated tools.

It is the first solution to allow for the automatic generation of the key documents that are necessary to demonstrate compliance with the CMMC framework. More than just documents to satisfy a compliance requirement, Compliance Manager provides factual evidence, expert advice, and direction to minimize or eliminate the risk of a data breach.

You can compare Compliance Manager for CMMC to getting a medical exam. Compliance Manager automates the 'lab tests' for the technology environment. It includes interview and survey features to gather information manually. In addition, it provides a recommended treatment plan.

You can learn more about the CMMC model at: <https://www.acq.osd.mil/cmmc/index.html>.

Compliance Manager for CMMC Assessment Overview

Compliance Manager for CMMC combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a CMMC Assessment, you will:

- Access and log in to the RapidFire Tools Portal
- Create a site and set up a project
- Install the Compliance Manager server on the target network
- Collect data from the target network using the Portal's guided To Do List
- Generate CMMC Assessment reports and documentation



Network Prerequisites for Assessment Scans

For a successful network scan:

1. **ENSURE ALL NETWORK ENDPOINTS ARE TURNED ON THROUGHOUT THE DURATION OF THE SCAN.** This includes PCs and servers. The scan can last several hours.
2. **CONFIGURE THE TARGET NETWORK TO ALLOW FOR SUCCESSFUL SCANS ON ALL NETWORK ENDPOINTS.** See ["Pre-Scan Network Configuration Checklist" on the next page](#) for configuration guidance for both Windows Active Directory and Workgroup environments.
3. **GATHER THE INFORMATION BELOW TO CONFIGURE YOUR SCANS FOR THE CLIENT SITE.** Work with the project Technician and/or your IT admin on site to collect the following:
 - **Admin network credentials** that have rights to use WMI, ADMIN\$, and File and Printer Sharing on the target network.
 - **Internal IP range** information to be used when performing internal scans.

Note: Compliance Manager will automatically suggest an IP range to scan on the network. However, you may wish to override this or exclude certain IP addresses.

- **External IP addresses** for the organisation to be used when setting up External Vulnerability Scans.
- **RapidFire Tools Portal User Credentials**
- For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IP address of the domain controller.
- For Windows Workgroup network environments, a list of the Computers to be included in the Assessment and the Local Admin Credentials for each computer.

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation – and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

Note: You must have the .NET 4.6.2 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
GPO Configuration for Windows Firewall (Inbound Rules)	
<input type="checkbox"/>	<p>Allow <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none">• Windows Management Instrumentation (ASync-In)• Windows Management Instrumentation (WMI-In)• Windows Management Instrumentation (DCOM-In)
<input type="checkbox"/>	<p>Allow <i>File and printer sharing</i> to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none">• File and Printer Sharing (NB-Name-In)• File and Printer Sharing (SMB-In)

Complete	Domain Configuration
	<ul style="list-style-type: none"> File and Printer Sharing (NB-Session-In)
<input type="checkbox"/>	<p>Enable <i>Remote Registry</i> “read only” access on computers targeted for scanning.</p> <p>Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.</p>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p> <ul style="list-style-type: none"> operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices to send ICMP echo reply messages in response to an ICMP echo request <p>Note: ICMP requests are used to detect active Windows computers and network devices to scan.</p>
GPO Configuration for Windows Services	
<input type="checkbox"/>	<p><i>Windows Management Instrumentation (WMI)</i></p> <ul style="list-style-type: none"> Startup Type: Automatic
<input type="checkbox"/>	<p><i>Windows Update Service</i></p> <ul style="list-style-type: none"> Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Registry</i></p> <ul style="list-style-type: none"> Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Procedure Call</i></p>

Complete	Domain Configuration
	<ul style="list-style-type: none"> Startup Type: Automatic
Network Shares	
<input type="checkbox"/>	<ul style="list-style-type: none"> <i>Admin\$</i> must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)
3rd Party Firewalls	
<input type="checkbox"/>	<ul style="list-style-type: none"> Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. <div> Note: This is a requirement for both Active Directory and Workgroup Networks. </div>

Checklist for Workgroup Environments

Before you perform a workgroup assessment, run the following PowerShell commands on the target network and the machine that will perform the scan. These three configurations should help you avoid most issues in a workgroup environment. Each command is followed by an explanation and link to Microsoft documentation.

1. `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`

By default, UAC only allows remote administration tasks to be performed by the Built-in Administrator account. To work around this, this command sets the LocalAccountTokenFilterPolicy registry key to 1. This allows any local admin to perform remote administrative tasks (i.e. access to system shares C\$, Admin\$, etc.).

<https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows>

2. `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes`

This command creates an Inbound firewall rule to allow access to the WMI service and namespaces.

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista>

3. `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`

This command creates an Inbound firewall rule which enables File and Printer Sharing on the machine. File and printer sharing is required in order to access the Admin\$ share on remote machines.

<https://answers.microsoft.com/en-us/windows/forum/all/turning-on-file-and-printer-sharing-windows-10/bb3066eb-f589-4021-8f71-617e70854354>

You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

Complete?	Workgroup Configuration
	Network Settings
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Admin\$</i> must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>File and printer sharing</i> must be enabled on the computers you wish to scan
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</i> <ul style="list-style-type: none"> • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call

Complete?	Workgroup Configuration
<input type="checkbox"/>	<ul style="list-style-type: none"> • Workgroup computer administrator user account credentials. <div data-bbox="443 363 1401 510"> <p>Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard.</p> </div>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p> <ul style="list-style-type: none"> • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request <div data-bbox="443 1003 1325 1108"> <p>Note: ICMP requests are used to detect active Windows computers and network devices to scan.</p> </div>

To complete a CMMC Assessment, follow these steps:

Step 1 — Add Organizations

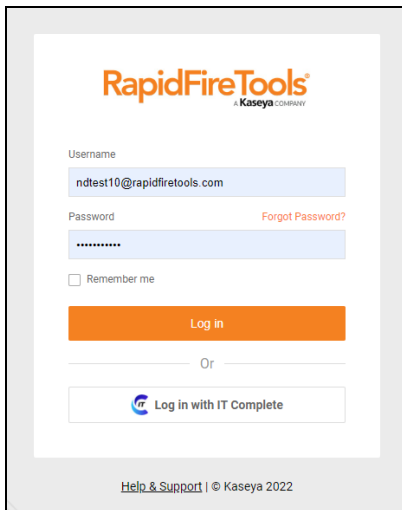
Before you begin your first IT or compliance assessment, you can optionally create an **organization**. Think of an organization as a folder in which you can store assessment projects for a particular client. For example, if a client has multiple sites or distinct networks that you want to assess individually, use an organization to keep these client sites in one neat container.

Tip: Much like folders in Windows Explorer, you can create multiple Organizations and can move your sites between them.

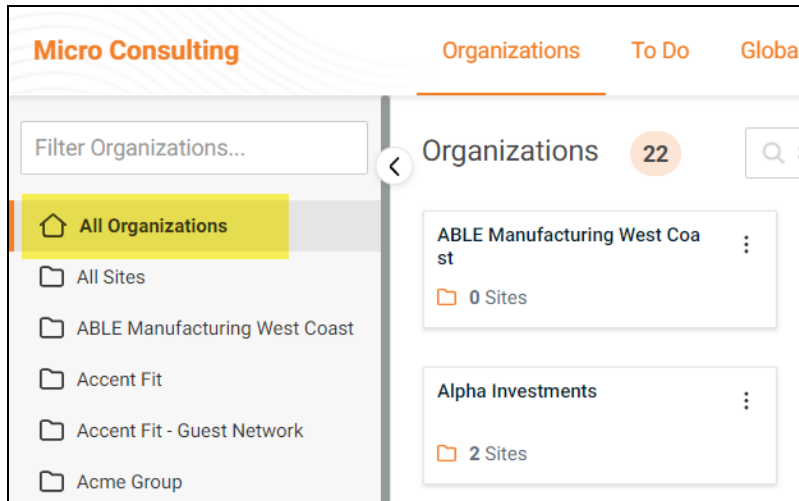
Add an Organization

To add an Organization:

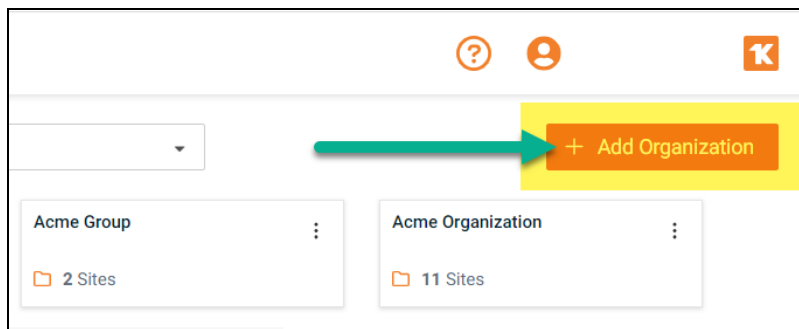
1. Access the RapidFire Tools Portal at <https://www.youritportal.com> and log in with your credentials.



2. Access the **Organizations** page from the top-menu. Select **All Organizations** from the side menu.



3. Then click **Add Organization**.



4. Enter an Organization name. For example, this might be the name of a large company for whom you want to create multiple sites and types of IT and compliance assessments. Then click **Confirm**.

Add Organization

Organization Name*

Add from IT Glue

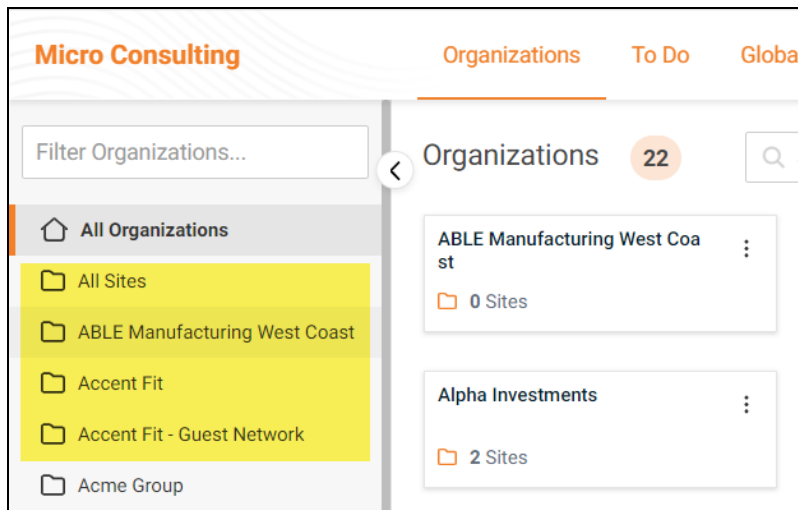
Grande Vista


Organization names must start with an alphanumeric character, may only include alphanumeric characters, dash, and space and must be less than 50 characters long.

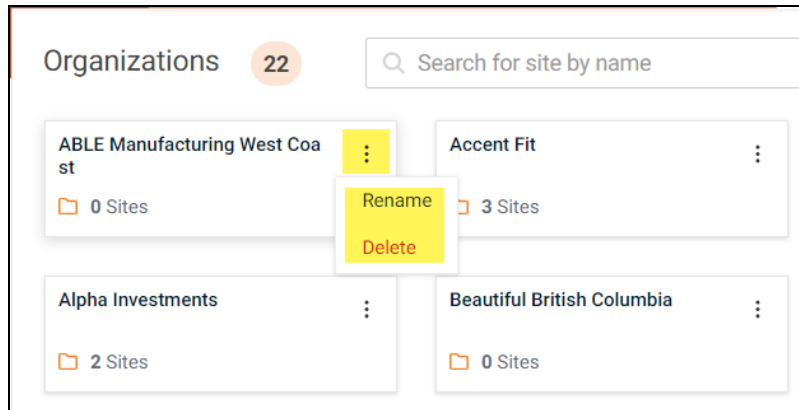
Cancel

Confirm

5. You can see each organization you've created from the left-side menu.



6. From the  button you can rename or delete the Organization. You can also see the number of sites grouped under the Organization.

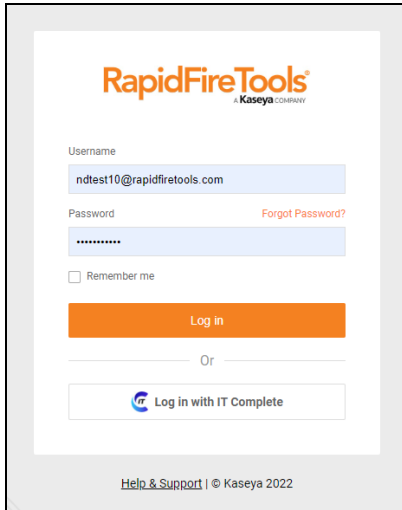


Step 2 — Create a New Site

Tip: We recommend you get started by making a "practice site" and running your first assessment in-house. Use this to familiarise yourself with Compliance Manager and the installation and configuration process.

The first step in performing a CMMC Assessment is creating a "Site". Sites help you organise your assessments. This task is performed by the Site Administrator. To create a site:

1. Access the RapidFire Tools Portal at <https://www.youritportal.com> and log in with your credentials.

The image shows the login page for RapidFireTools, a Kaseya company. The page has a white background with a light gray border. At the top, the logo "RapidFireTools" is in orange, with "A Kaseya COMPANY" in smaller text below it. Below the logo, there are two input fields: "Username" with the text "ndtest10@rapidfiretools.com" and "Password" with a masked password "*****". A "Forgot Password?" link is to the right of the password field. Below the password field is a checkbox labeled "Remember me". A large orange "Log in" button is centered below the checkbox. Below the button is a horizontal line with the word "Or" in the center. Below the line is a button with the IT Complete logo and the text "Log in with IT Complete". At the bottom, there is a link "Help & Support" and a copyright notice "© Kaseya 2022".

Username
ndtest10@rapidfiretools.com


Password

[Forgot Password?](#)

☐ Remember me

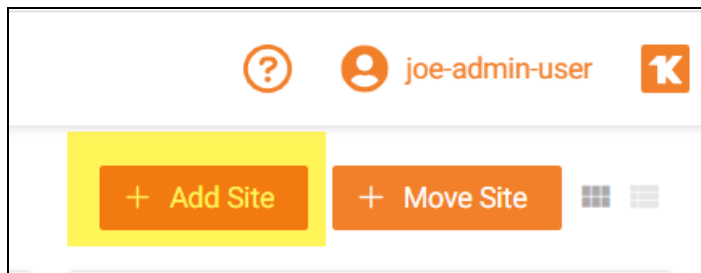
Log in

Or

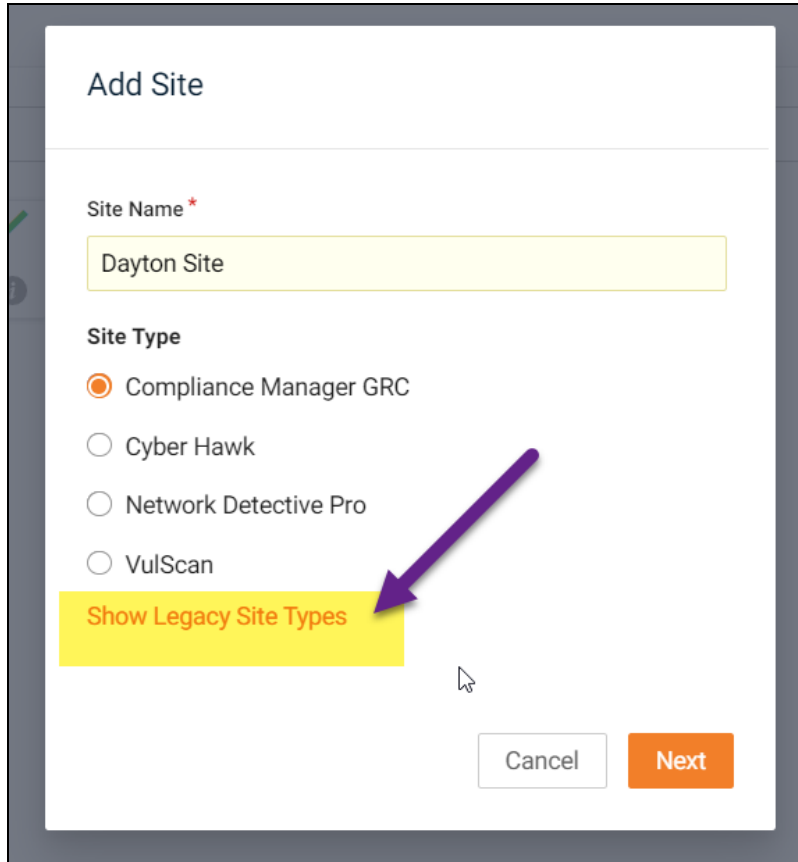
 Log in with IT Complete

[Help & Support](#) | © Kaseya 2022

2. From the Sites page, click **Add Site**.



3. Enter a **Site Name**. This can be the name of the client for whom the assessment is being performed, for example.
4. Under **Site Type**, select **Show Legacy Site Types**.



Add Site

Site Name *

Dayton Site

Site Type

☒ Compliance Manager GRC

☐ Cyber Hawk

☐ Network Detective Pro

☐ VulScan

Show Legacy Site Types

Cancel Next

5. Select **Compliance Manager (Legacy)** and then select your assessment type.
- If you wish to perform a EU GDPR assessment, select **EU GDPR**.
 - If you wish to perform a UK GDPR assessment, select **UK GDPR**.
 - If you wish to perform a HIPAA assessment, select **HIPAA**.
 - If you wish to perform a Cyber Insurance assessment, select **Cyber Insurance**.
 - If you wish to perform a NIST CSF assessment, select **NIST**.
 - If you wish to perform a CMMC/NIST 800-171 assessment, select **CMMC/NIST 800-171**.

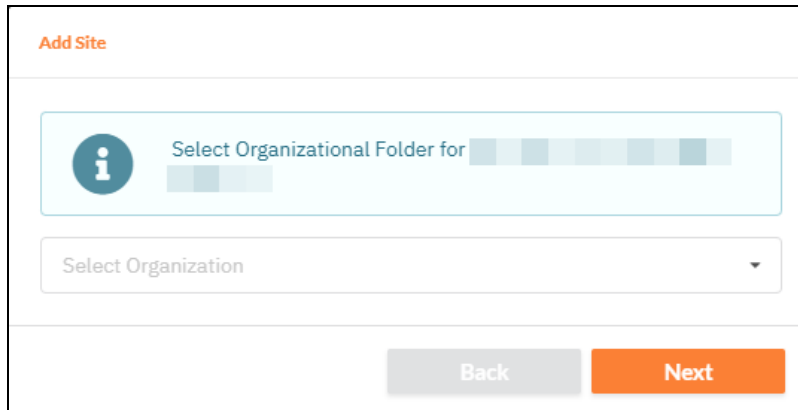
Add Site

Site Type

- ☐ Compliance Manager GRC
- ☐ Cyber Hawk
- ☐ Network Detective Pro
- ☐ VulScan
- ☒ Compliance Manager (Legacy)

- ☐ EU GDPR
- ☐ UK GDPR
- ☐ HIPAA
- ☐ Cyber Insurance
- ☐ NIST CSF
- ☐ CMMC / NIST 800-171

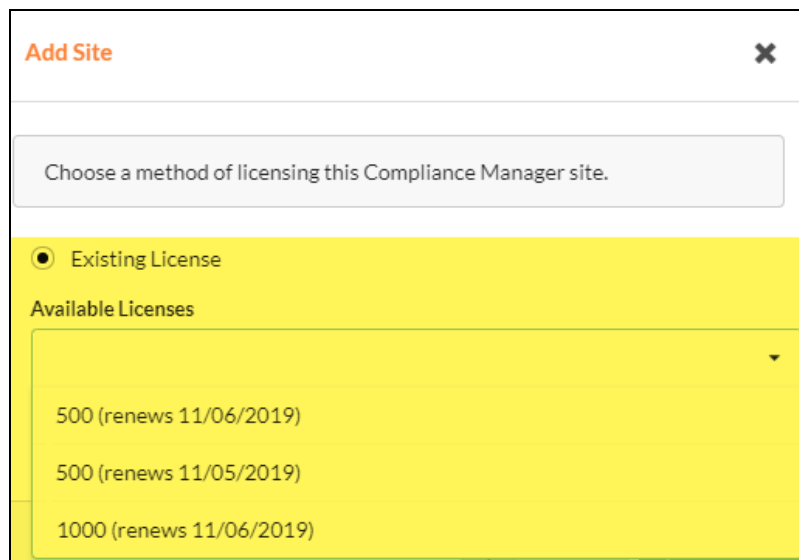
6. Click **Next**. Select an **Organization Folder** for the new site.



The screenshot shows a web form titled "Add Site". It contains a light blue box with an information icon and the text "Select Organizational Folder for" followed by a series of colored squares. Below this is a dropdown menu labeled "Select Organization". At the bottom are "Back" and "Next" buttons.

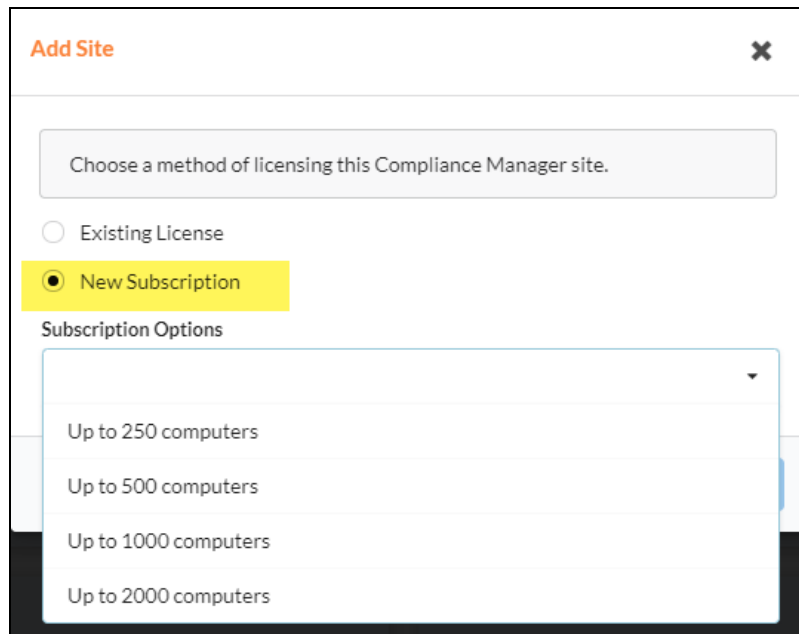
7. Select a subscription option (MSP only). You can choose to:

- a. Use an **Existing License** you have purchased previously. Select the existing license from the drop-down menu and click **Next**.



The screenshot shows the "Add Site" form with a close button (X) in the top right. A message box says "Choose a method of licensing this Compliance Manager site." Below it, the "Existing License" option is selected with a radio button. Under "Available Licenses", a dropdown menu is open showing three options: "500 (renews 11/06/2019)", "500 (renews 11/05/2019)", and "1000 (renews 11/06/2019)".

- b. Create a **New Subscription**. Select the subscription option from the drop-down menu and click **Next**.



Add Site [X]

Choose a method of licensing this Compliance Manager site.

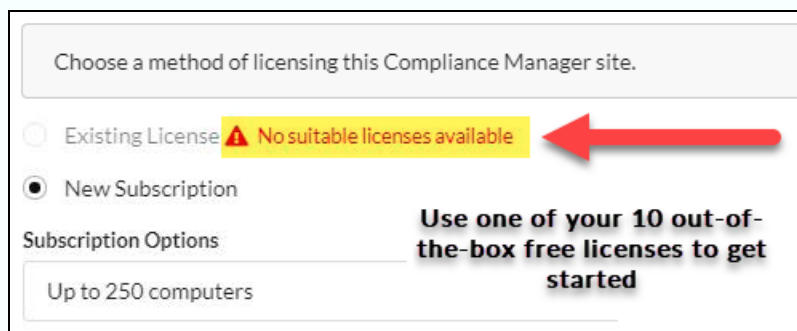
☐ Existing License

☒ **New Subscription**

Subscription Options

- Up to 250 computers
- Up to 500 computers
- Up to 1000 computers
- Up to 2000 computers

Note: You have **10 FREE** Site licenses as part of your initial Compliance Manager subscription. Each of these licenses can cover a site with up to 250 computers. *Select one of these free licenses for use with your first 10 new Sites.* We suggest that you use 1 of the 10 licenses for your own internal use, such as familiarizing yourself with the product and assessment processes.



Choose a method of licensing this Compliance Manager site.

☐ Existing License **⚠ No suitable licenses available**

☒ New Subscription

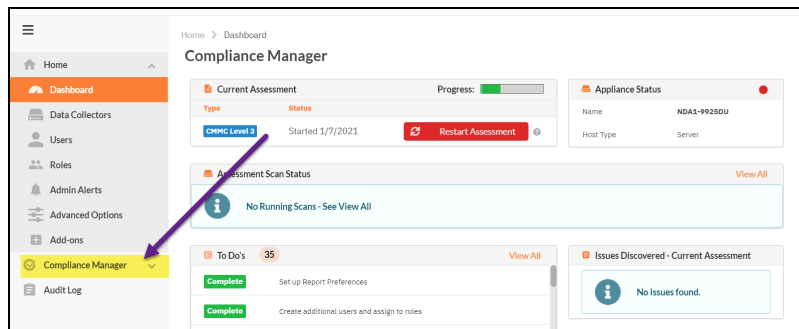
Subscription Options

- Up to 250 computers

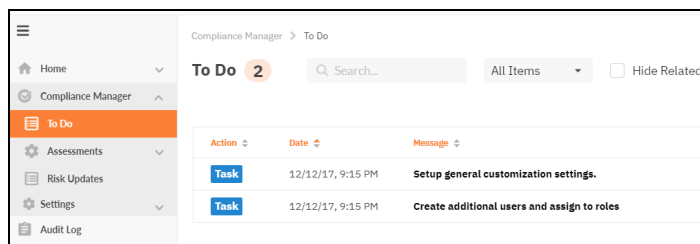
Use one of your 10 out-of-the-box free licenses to get started

If you wish to purchase additional licenses or upgrade to a higher license (500 and above), you will be billed extra. Contact your Sales Representative for more details.

8. The Site Home page will appear. Click the **Compliance Manager** tab.



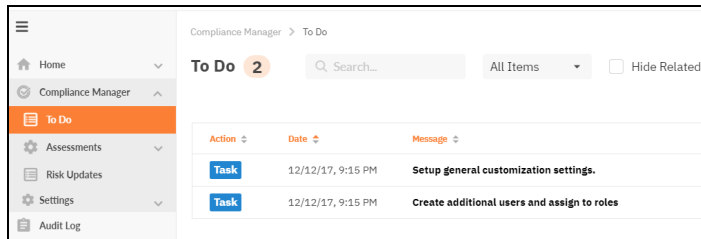
The Site To Do page will appear.



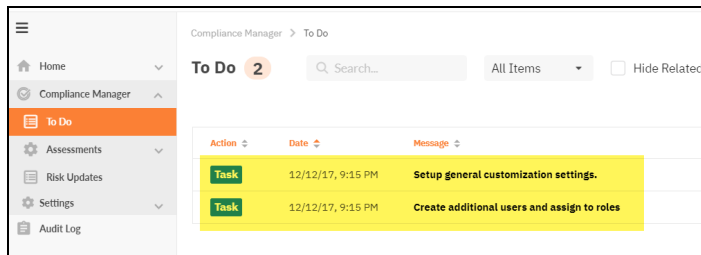
Step 3 — Use the To Do List to Complete Tasks

The **To Do List** will guide you through the CMMC Assessment process. It presents the tasks you need to complete for the assessment. To use the To Do List:

1. From the **[Your Site] > Compliance Manager** tab, click **To Do**.



The Site's To Do list will appear.



2. Click on a To Do item to open more detailed information and instructions about each step in the assessment process.

Tip: The Tasks steps in this quick start guide walk you through each To Do task. Note that the tasks may appear in a different order depending on which tasks you complete first.

Re-run or Modify To Do Items

Some to do items can be re-run or modified after they have been completed.

- Automated Scans can be re-run directly from the To Do item. Re-running a scan will reset whatever forms were generated from that can. Any data entered into those forms during the current assessment will be lost. The worksheets will reappear as

new To Do items.

- Worksheets and forms can be modified directly from the To Do item.

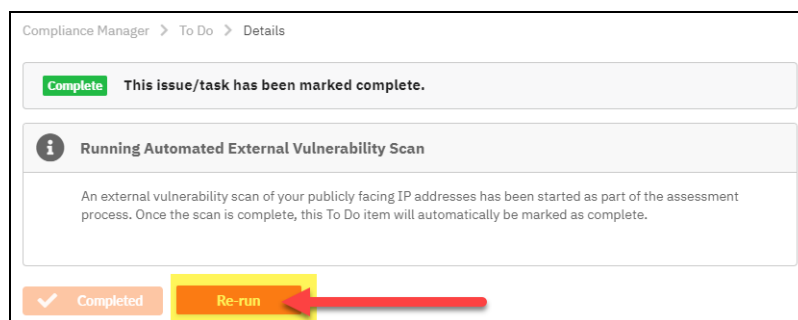
To re-run or modify a To Do item:

1. Open a completed To Do item from the To Do list.

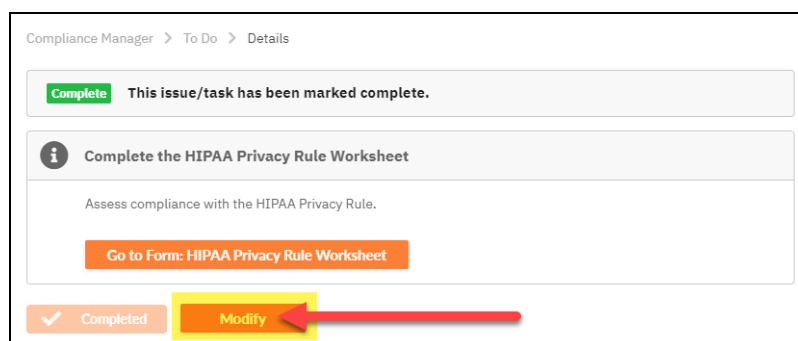
Complete	12/10/18, 2:49 PM	Install the Compliance Manager Server Software
Complete	11/5/19, 6:58 PM	Start HIPAA Assessment
Complete	11/5/19, 6:58 PM	Type of HIPAA Assessment
Complete	11/5/19, 6:58 PM	Running Automated External Vulnerability Scan
Task	11/5/19, 6:58 PM	Running Pre-scan Analysis

2. Depending on the type of To Do item (scan or worksheet), select **Re-run** or **Modify**:

- If the To Do item is an automated scan, click **Re-run**.



- If the To Do item is a Worksheet or Survey, click **Modify**.



3. A list of related To Do items that will be reset will appear. Confirm that you wish to proceed.

Note: For example, if you reset an automated scan, 1) any worksheets that contain data from that scan will also be reset and 2) any data previously entered in that form during the current assessment will be lost.

Warning

Re-running the currently completed step will invalidate the following items:

- Complete External Port Use Worksheet

Proceed?

OK Cancel

4. Once you reset or modify the To Do item, the regenerated item will appear in the To Do list.

Complete	11/11/19, 2:30 PM	Type of HIPAA Assessment
Complete	11/12/19, 1:55 PM	Complete the HIPAA Privacy Rule Worksheet
Task	11/12/19, 1:55 PM	Complete the HIPAA Breach Notification Rule Worksheet
Task	11/26/19, 8:25 AM	Running Automated External Vulnerability Scan

Assessment Progress Bar

From the Site Dashboard, you can view a progress bar for your assessment. This progress bar is advanced when you complete assessment tasks.

Home > Dashboard

Compliance Manager

Current Assessment

Type	Status
HIPAA	Started 2/24/2021

Progress: 14 of 27

Restart Assessment

Appliance Status

Name	Host Type
NDA3-657	Server

Assessment Scan Status

Scan Type	Status	Start Date UTC	End Date UTC	Last Scan Details
Deep Scan	Failed	08-Mar-2021 7:35:59 PM	-	Unable to scan any remote computers (ref #18314363)

To Do's 15 [View All](#) **Issues Discovered - Current As**

If you hover over the progress, you can see the number of To Do items remaining in the assessment. This number is based on the total steps in the assessment, rather than the

current To Do list. Once all To Do items are completed, the Progress Bar will be removed from the Current Assessment panel in the Compliance Manager Dashboard.

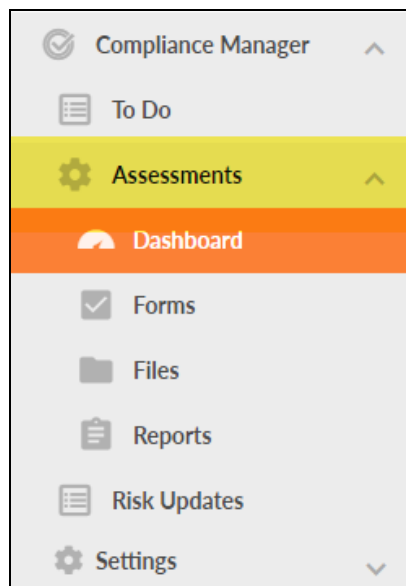
Step 4 — Set Up the CMMC Assessment Project

I. **Task** Set Up Report Preferences.

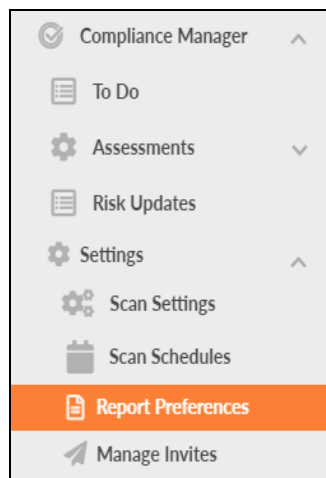
Compliance Manager generates **assessment reports** and **proof of compliance documents** to help you complete your CMMC Assessment. You can also customize these reports to align with your company or organisation branding guidelines and information. This task is performed by an Administrator.

To configure Report Preferences:

1. From your Site Home Page, go to **Compliance Manager > Settings**.



Next, click **Report Preferences** to access the customization settings. This includes company information, images, and design elements for this site's reports.



2. Customize your reports. This includes company information, images, and design elements for this site's reports.

A screenshot of the 'Report Preferences' configuration page. The breadcrumb trail at the top reads 'Compliance Manager GRC / Settings / Report Preferences'. The page title is 'Report Preferences'. Below the title are four tabs: 'Text' (selected and underlined in orange), 'My Logo', 'Theme', and 'Cover Image'. The 'Text' tab contains four input fields: 'Report Prepared For:' with the value 'Advent Technologies'; 'Report Prepared By:' with the value 'Micro Consulting'; 'Footer:' with the value 'PROPRIETARY & CONFIDENTIAL'; and 'Cover Page Disclaimer:' with a text area containing a confidentiality note: 'CONFIDENTIALITY NOTE: The information contained in this report d of the client specified above and may contain confidential, privileged information. If the recipient of this report is not the client or address prohibited from reading, photocopying, distributing or otherwise usin any way.'

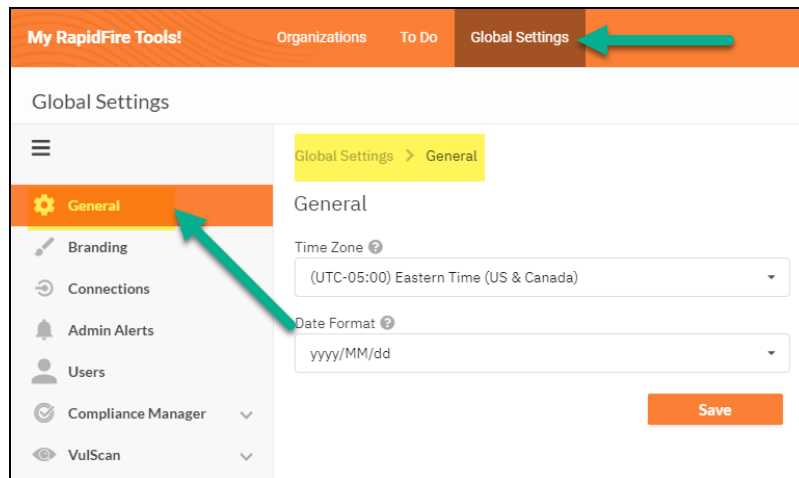
3. Once you finish configuring Report Preferences, return to the item in the To Do list and click **Mark Complete**. Do this each time you complete a task in the To Do list.



II. *Recommended:* **Set Time Zone.**

You can set your time zone from **Global Settings > General**. Set your time zone to schedule automated scans at your preferred local time. To configure time zones:

1. Go to **Global Settings > General**.



2. Select your time zone from the drop down menu.
3. Click **Save**.

Note that the time zone setting is relatively narrow in scope. For example, To Do task creation time is shown based on your browser's local time, *not* the time zone setting in Global Settings. The time zone setting effects a few items, including:

- start time for scans when using the limit scan start time feature for a site
- last modified date of risk update reports
- last sync date and time for Kaseya BMS billing integration

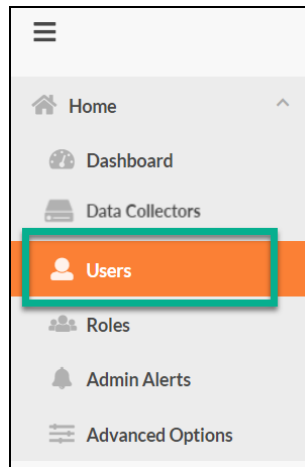
III. **Task** **Create additional users and assign to roles.**

Your CMMC Assessment has several roles: these include **Site Administrator**, **Technician**, **Internal Auditor**, and (optional) **Subject Matter Expert (SME)**. Each role performs different tasks within the assessment.

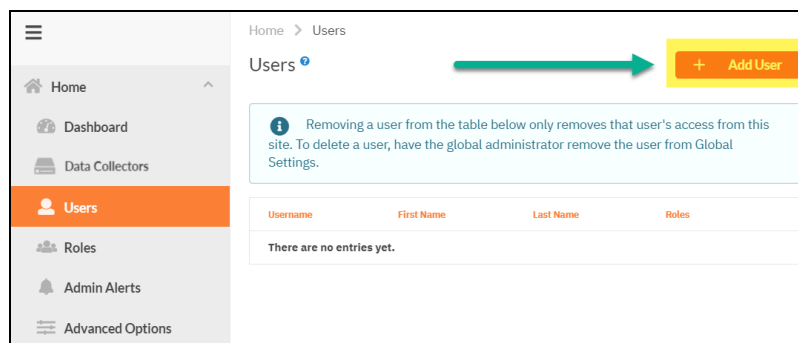
Tip: Before you begin the assessment, you will need to assign users to each role except the optional SME role. This allows users to be assigned assessment tasks within their To Do list and email notifications.

This task is performed by the Site Administrator. To assign users to project roles:

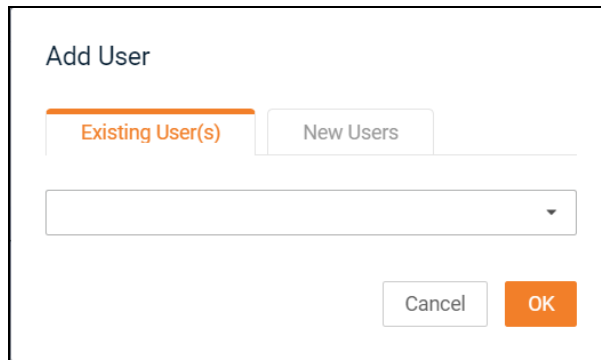
1. From the Home page for your Site, click **Users**.



2. Click **Add User**.



- i. Add **Existing Users(s)** by searching for their user name within the drop-down menu.

A dialog box titled "Add User" with two tabs: "Existing User(s)" (selected) and "New Users". Below the tabs is a text input field. At the bottom are "Cancel" and "OK" buttons.

Add User

Existing User(s) New Users

Cancel OK

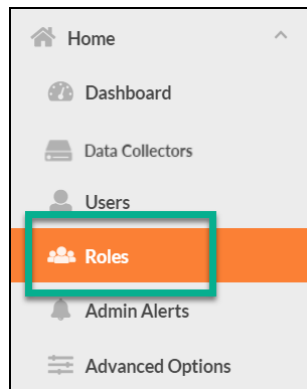
- ii. Alternatively, you can create a **New User** account to provide individuals access to the Portal and assessment process. You will need to enter an email address, first and last name, and password for each user. The email address you enter is where the user will receive To Do Notifications from Compliance Manager.

Important: Send new users their login credentials after you add them to the site.

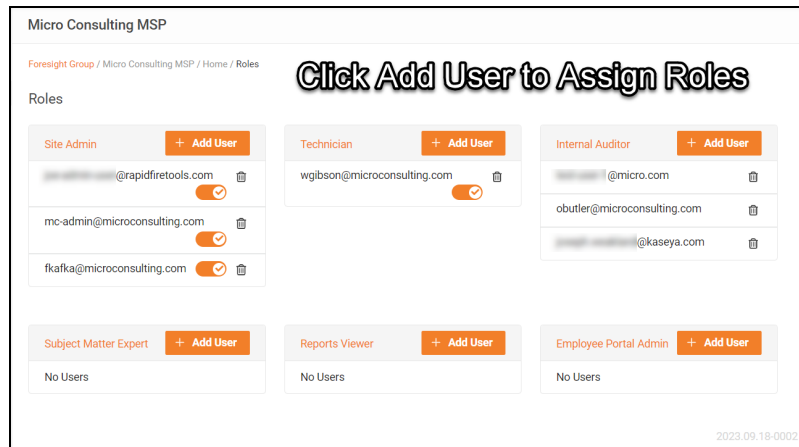
- iii. Click **Add** to add the user to the site.

Next you will associate these new users with your CMMC Assessment Site. To do this:

- 3. From the Home tab side menu, click **Roles**.

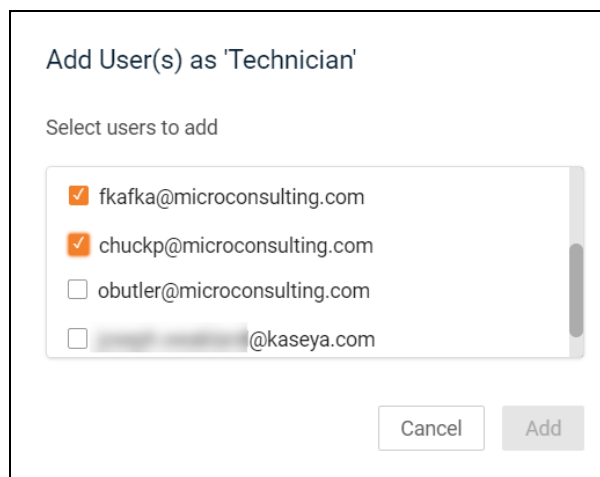


4. Next to each role, click **Add User** to assign users to the **Technician**, **Internal Auditor**, and (optional) **Subject Matter Expert (SME)** roles. The users assigned to these roles will receive assessment task notifications for that role.



5. Select each user you wish to assign to the role. Then click **Add**.

Note: Before you can assign a user a Role, you must first create that user and/or associate them with your Site.



Important: Do not assign the SME role to users with other role assignments. Doing so will limit their access to the portal.

6. When you have finished adding users to your site and assigning roles, click **Mark Complete** on the task To Do page.

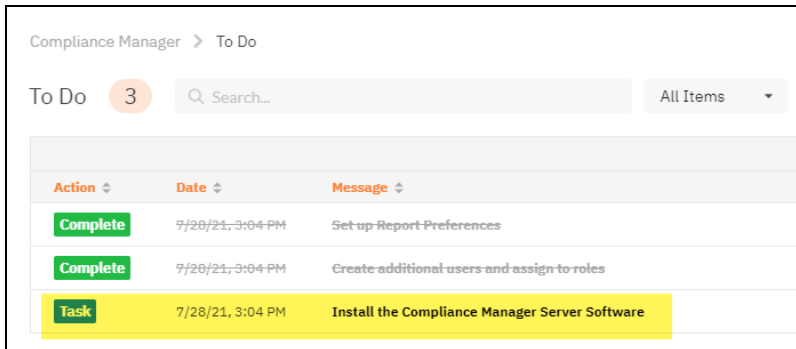


Important: Be sure to send the users their login credentials in order to access the RapidFire Tools Portal and begin working on assessment tasks.

Step 5 — Install and Configure the Compliance Manager Server

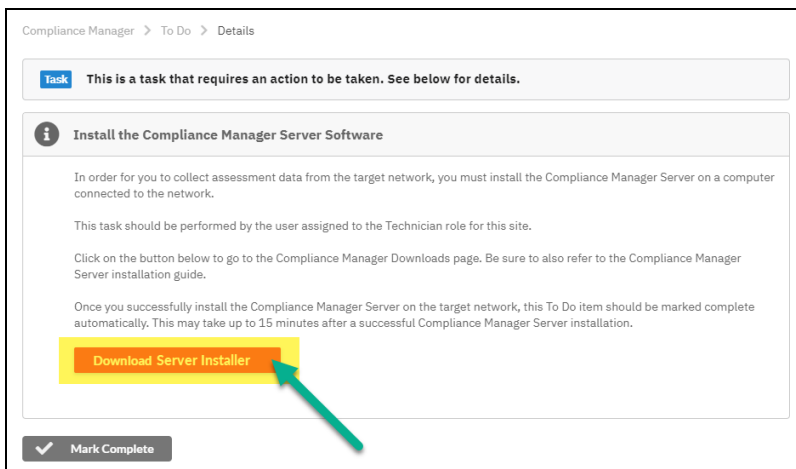
I. **Task** Install Compliance Manager Server.

Install the **Compliance Manager Server** on the target network. *This task is performed by the Technician.* The Server collects data and performs automated scans within the assessment environment.



Compliance Manager > To Do		
To Do	3	Q Search...
All Items ▾		
Action ▾	Date ▾	Message ▾
Complete	7/28/21, 3:04 PM	Set up Report Preferences
Complete	7/28/21, 3:04 PM	Create additional users and assign to roles
Task	7/28/21, 3:04 PM	Install the Compliance Manager Server Software

Click **Download Server Installer** to visit <https://www.rapidfiretools.com/cm>. Refer to the separate **Compliance Manager Server Installation Guide** for more detailed instructions.



Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

i **Install the Compliance Manager Server Software**

In order for you to collect assessment data from the target network, you must install the Compliance Manager Server on a computer connected to the network.

This task should be performed by the user assigned to the Technician role for this site.

Click on the button below to go to the Compliance Manager Downloads page. Be sure to also refer to the Compliance Manager Server installation guide.

Once you successfully install the Compliance Manager Server on the target network, this To Do item should be marked complete automatically. This may take up to 15 minutes after a successful Compliance Manager Server installation.

Download Server Installer

✓ Mark Complete

Important: You can only install **one** RapidFire Tools server/appliance on a PC or endpoint at a time. If you need to install multiple server(s)/appliance(s), install each one on a separate endpoint on the network.

Note: Once you install the Server, this To Do item will automatically be marked complete. **This may take several minutes.**

II. **Task** Configure Server Scan settings.

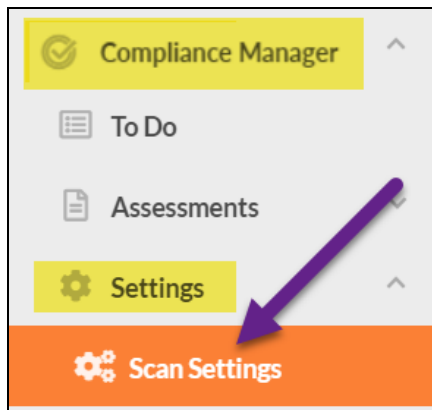
Before you configure scan settings, first determine if the target network is an Active Directory Domain OR a Workgroup. Then refer to the instructions below.

- Look here to ["Configure Scan Settings for Active Directory Domain" below](#)
- Look here to ["Configure Scan Settings for Workgroup" on page 42](#)

Tip: For best results, be sure to follow ["Pre-Scan Network Configuration Checklist" on page 134](#).

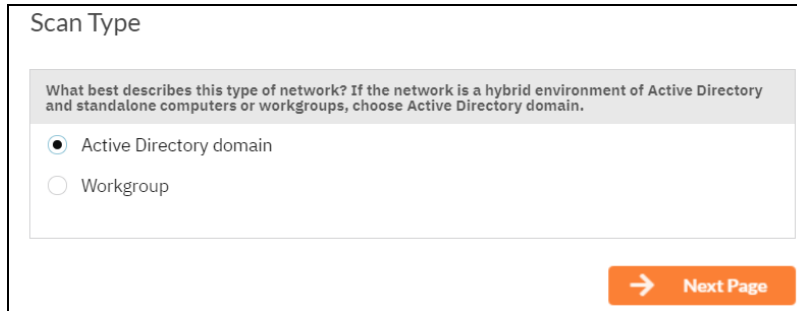
Configure Scan Settings for Active Directory Domain

Set the **Scan Settings** from the [Your Site] > **Compliance Manager** > **Settings** > **Scan Settings** page. Complete all required prompts. This task is performed by the Technician.

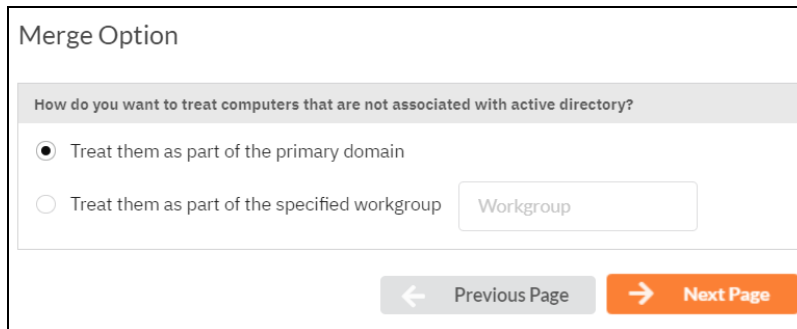


Follow the steps below to configure the Scan Settings for the Compliance Manager Server:

1. Select the Scan Type: **Active Directory Domain**. Click **Next Page**.



2. The **Merge Options** page will appear. Configure how you wish to treat computers that are not associated with Active Directory. You can choose to:



- a. Treat them as part of the primary domain
- b. Treat them as part of a specific workgroup by entering a workgroup name

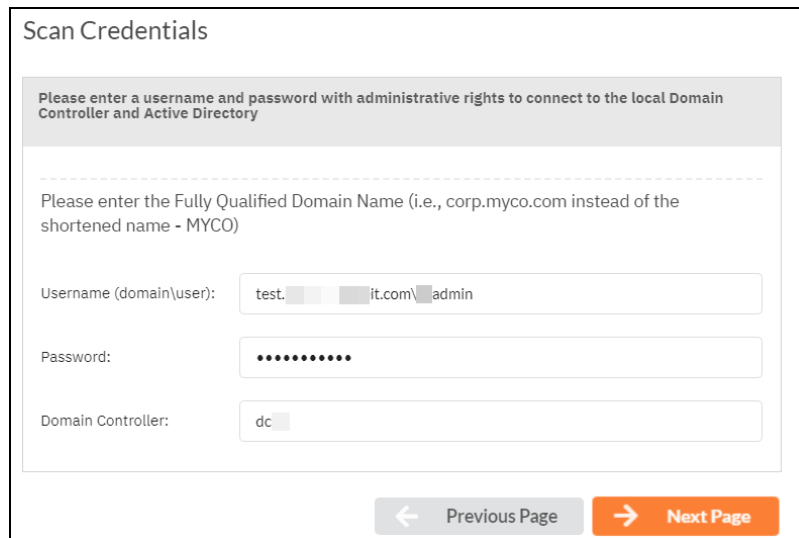
Tip: Use this feature to tell Compliance Manager how to handle computers that are not connected to the domain. This will help those computers appear where you want them when you generate reports at the end of the assessment.

Select a merge option and click **Next Page**.

3. Enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory.

Note: Be sure to enter the Fully Qualified Domain Name (FQDN) name before the username. Example: **corp.myco.com\username**.

4. Also enter the name or IP address of the Domain Controller. Click **Next Page** to test a connection to the local Domain Controller and Active Directory to verify your credentials.



Scan Credentials

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory

Please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name - MYCO)

Username (domain\user): test.it.com\admin

Password:

Domain Controller: dc

← Previous Page Next Page →

5. The **Local Domains** window will appear. If you wish to scan only specific domains or OUs, select those here. Click **Next Page**.

Local Domains

Below is a list of the detected domains in the current forest of Active Directory

☒ Gather Information for ALL the domains detected.

☐ Gather Information for only the Domains and OUs selected below.

- ☐ test.performanceit.com
 - ☐ BuiltIn
 - ☐ Computers
 - ☐ Domain Controllers
 - ☐ ForeignSecurityPrincipals
 - ☐ Keys
 - ☐ Managed Service Accounts
 - ☐ Program Data
 - ☐ Microsoft
 - ☐ System
 - ☐ TEST
 - ☐ Users

[< Previous Page](#) [Next Page >](#)

6. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.

Additional Credentials

Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

Username:

Password:

+ Add Remove Selected Entry

test.performanceit.com\jwadmin (AD user to be used first)

← Previous Page Next Page →

7. The **IP Ranges** screen will then appear. The Compliance Manager server will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

YOU MUST ENTER AN IP RANGE TO PERFORM THE SCAN.

IP Ranges ?

Auto-Detected IP Ranges on Remote Appliance

10.

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

+ Add

10.

Exclude IPs

Reset to Auto-Detected

Remove Selected Entry

Clear All Entries

← Previous Page

Next Page →

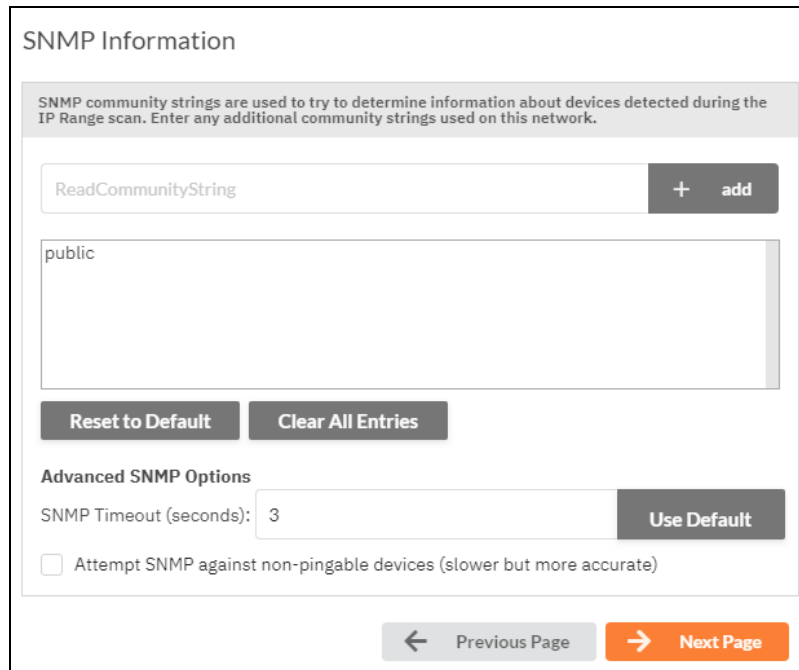
From this screen you can also:

- Click **Reset to Auto-detected** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

Note: Key network component IP addresses should be excluded in order to prevent scans being performed from impacting the performance of a device when it is being scanned. For example, a company might want to exclude the IP Address range for their voice over IP telephone system if they are performing a scan during business hours.

Click **Next Page** once you have configured the IP ranges for the scan.

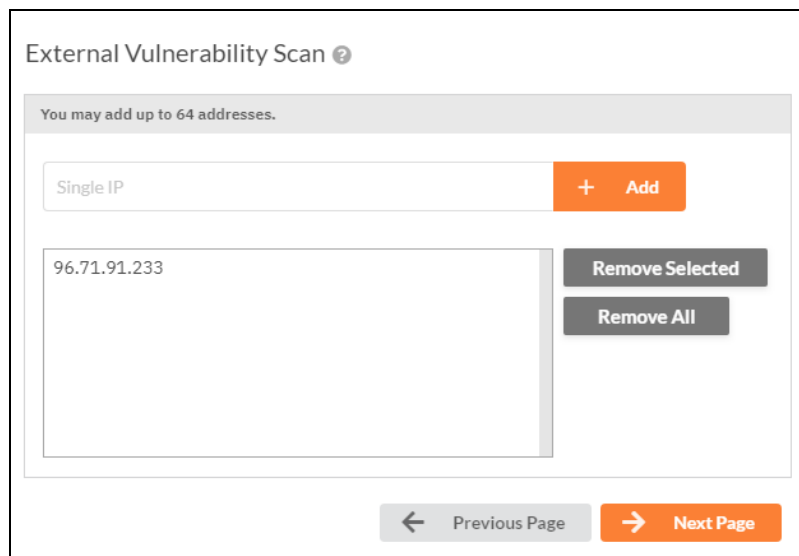
8. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.



9. Enter the IP addresses for the external vulnerability scan. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Note: IP ranges for the external vulnerability scan are not supported at this time. Please enter individual IPs for the external scan.



External Vulnerability Scan ?

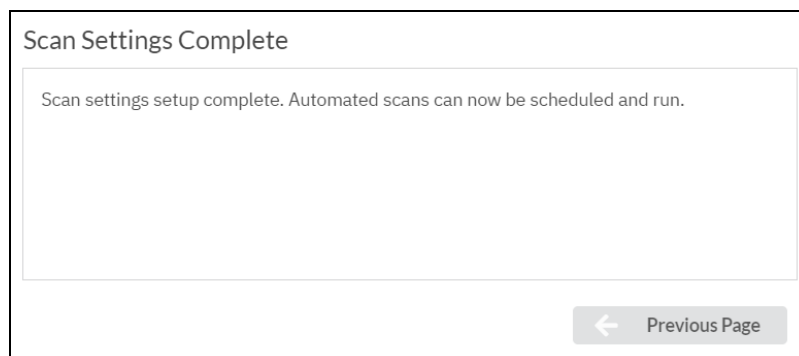
You may add up to 64 addresses.

Single IP + Add

96.71.91.233 Remove Selected
Remove All

← Previous Page Next Page →

10. Your scan settings will then be complete. Return to the To Do list and continue assessment tasks.



Scan Settings Complete

Scan settings setup complete. Automated scans can now be scheduled and run.

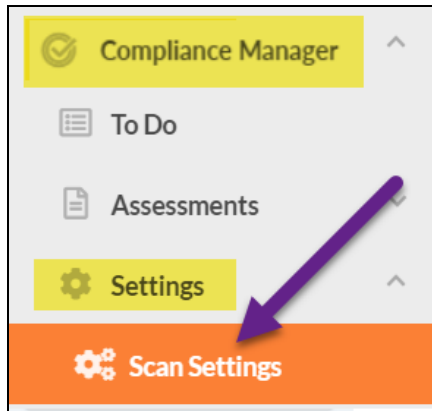
← Previous Page

Note: Stepping through the prompts creates the Scan Settings. Once the settings are saved, the Start CMMC Assessment To Do item is what is used to trigger the scans.

When you have finished entering the scan settings, return to the To Do item and click **Mark Complete**.

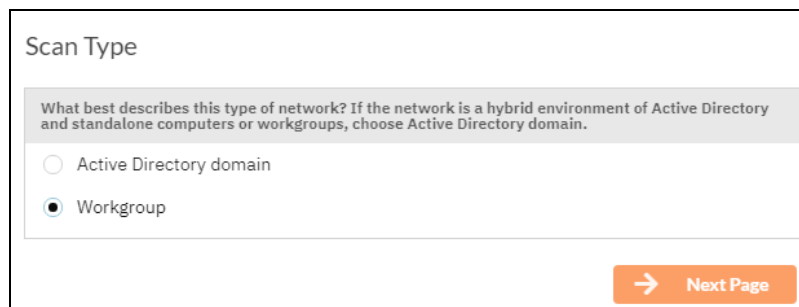
Configure Scan Settings for Workgroup

Set the **Scan Settings** from the **[Your Site] > Compliance Manager > Settings > Scan Settings** page. Complete all required prompts. This task is performed by the Technician.



Follow the steps below to configure the Scan Settings for the Compliance Manager Server:

1. From the Scan Settings screen, select the Scan Type: **Workgroup**. Click **Next Page**.



2. The **Merge Options** page will appear. Configure how you wish to treat computers that are not associated with Active Directory. You can choose to:

Merge Option

How do you want to treat computers that are not associated with active directory?

☒ Treat them as part of the primary domain

☐ Treat them as part of the specified workgroup

[< Previous Page](#) [Next Page >](#)

- a. Treat them as part of the primary domain
- b. Treat them as part of a specific workgroup by entering a workgroup name

Select a merge option and click **Next Page**.

3. Enter scan credentials with administrative rights to connect to the local computers in the workgroup.

Scan Credentials

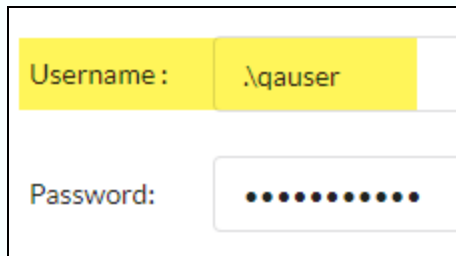
Please enter a username and password with administrative rights to connect to the local computers. Additional users and passwords can be added in the Additional Credentials screen.

Username :

Password:

[< Previous Page](#) [Next Page >](#)

Note: For Workgroups, you have two options for how to enter the username. First, you can enter the characters ".\" (without quotation marks) immediately before the username, as in the image below.



Username : .\quser

Password:

Second, you can optionally use the following format:
"computername\localuseraccountname." For example, "WGWINX\user."



Username : QWERTY\quser

Password:

If you have trouble connecting when using one username format, use the other format presented here.

Click **Next Page** to test the connection and verify your credentials.

4. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.

Important: If each workgroup PC has its own unique Admin username and password credentials, you will need to enter each set of credentials here in order to scan these PCs.

Additional Credentials

Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

Username:

Password:

+ Add Remove Selected Entry

test.performanceit.com\jwadmin (AD user to be used first)

← Previous Page Next Page →

5. The **IP Ranges** screen will then appear. The Compliance Manager server will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

YOU MUST ENTER AN IP RANGE TO PERFORM THE SCAN.

IP Ranges ?

Auto-Detected IP Ranges on Remote Appliance

10.

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

+ Add

10.

Exclude IPs

Reset to Auto-Detected

Remove Selected Entry

Clear All Entries

← Previous Page

Next Page →

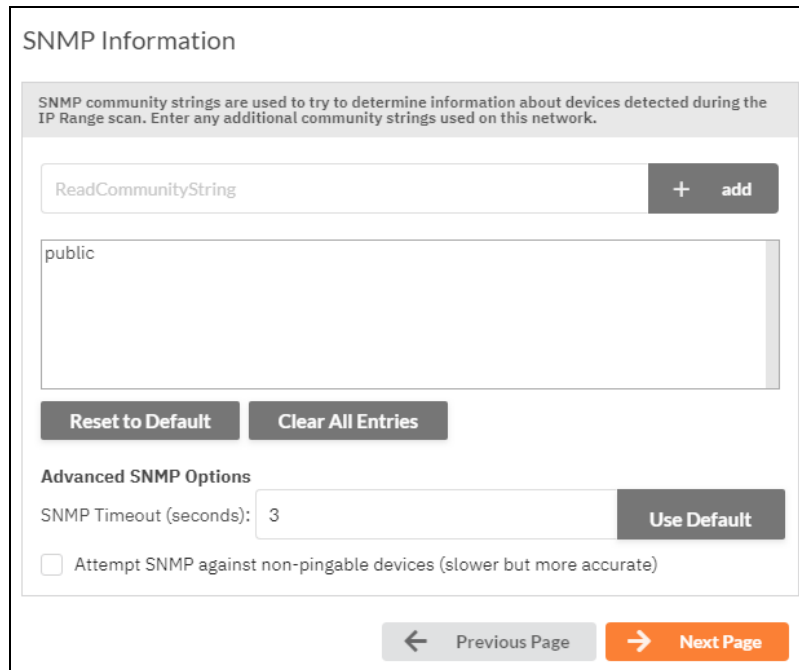
From this screen you can also:

- Click **Reset to Auto-detected** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

Note: Key network component IP addresses should be excluded in order to prevent scans being performed from impacting the performance of a device when it is being scanned. For example, a company might want to exclude the IP Address range for their voice over IP telephone system if they are performing a scan during business hours.

Click **Next Page** once you have configured the IP ranges for the scan.

6. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.



7. Enter the IP addresses for the external vulnerability scan. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Note: IP ranges for the external vulnerability scan are not supported at this time. Please enter individual IPs for the external scan.

External Vulnerability Scan ?

You may add up to 64 addresses.

Single IP + Add

96.71.91.233 Remove Selected
Remove All

← Previous Page Next Page →

8. Your scan settings will then be complete. Return to the To Do list and continue assessment tasks.

Scan Settings Complete

Scan settings setup complete. Automated scans can now be scheduled and run.

← Previous Page

Note: Stepping through the prompts creates the Scan Settings. Once the settings are saved, the Start CMMC Assessment To Do item is what is used to trigger the scans.

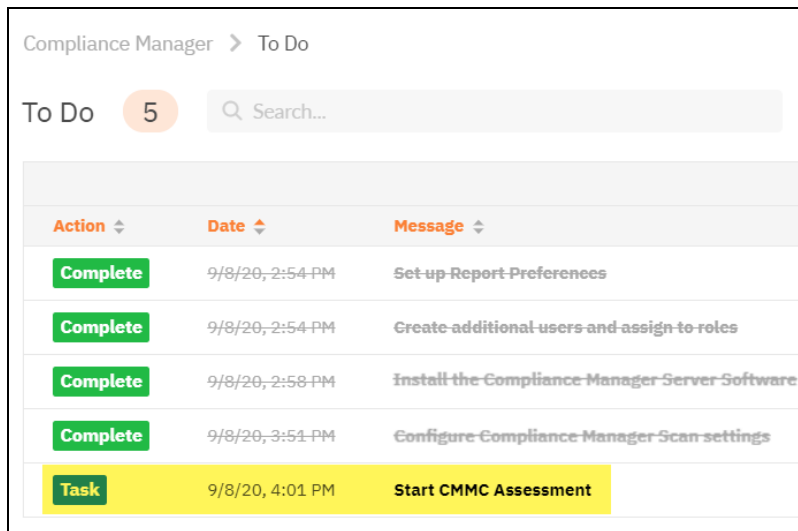
When you have finished entering the scan settings, return to the To Do item and click **Mark Complete**.

Step 6 — Start Assessment and Perform Pre-Scan Analysis

Note: The order of To Do tasks may appear differently in your assessment, depending on the order in which you or other users complete To Do tasks.

I. **Task** Start CMMC Assessment.

To begin performing the CMMC Assessment, click on the **Start CMMC Assessment** task from the To Do list:



Compliance Manager > To Do		
To Do	5	Search...
Action	Date	Message
Complete	9/8/20, 2:54 PM	Set up Report Preferences
Complete	9/8/20, 2:54 PM	Create additional users and assign to roles
Complete	9/8/20, 2:58 PM	Install the Compliance Manager Server Software
Complete	9/8/20, 3:51 PM	Configure Compliance Manager Scan settings
Task	9/8/20, 4:01 PM	Start CMMC Assessment

When you are ready to perform your first initial CMMC Assessment, click **Start Assessment**.

Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

i Start CMMC Assessment

When you are ready to perform your CMMC assessment, press the Start Assessment button. This will initiate both an internal pre-scan analysis and external vulnerability scan on the target network. It will also create a series of worksheets, which you can complete now or later. Once the automated scans are completed, additional worksheets may be created.

Start Assessment

✓ Mark Complete

Note: Completing this task will create several new assessment tasks in the To Do list. The task **Type of CMMC Assessment** will be added, where you can choose whether to add additional worksheets for an expanded CMMC assessment. Two scans that will begin automatically: the **Pre-Scan** and the **External Vulnerability Scan**. The scans will be marked complete automatically when they finish.

II. **Task (Automated) Running the Automated External Vulnerability Scan.**

The assessment includes an external vulnerability scan of your publicly facing IP addresses.

Task	5/14/19, 11:00 AM	Running Automated External Vulnerability Scan
-------------	-------------------	---

Once the scan is complete, this To Do item will automatically be marked as complete.

Task This is a task that requires an action to be taken. See below for details.

☒ **Running Automated External Vulnerability Scan**
An external vulnerability scan of your publicly facing IP addresses has been started as part of the assessment process. Once the scan is complete, this To Do item will automatically be marked as complete.

☒ Mark Complete

Note: New worksheets will appear once the External Vulnerability scan completes.

III. **Task** Running Pre-Scan Analysis.

In this task, the Compliance Manager server will begin an automated pre-scan analysis of the target network.

Task 5/14/19, 11:00 AM Running Pre-scan Analysis

This will verify the credentials and attempt to detect issues to ensure you have the most accurate automated scans.

Task This is a task that requires no action to be taken, and will automatically complete on its own.

☒ **Running Pre-scan Analysis**
A pre-scan analysis of your network has been started. This will verify the credentials and attempt to detect issues to ensure you have the most accurate automated scans. If issues are identified, you may follow the recommended corrective actions and re-run this analysis.

When the automated scan is completed, and any issues are identified, you may follow the recommended corrective actions and re-run this analysis.

IV. **Task** Review Pre-Scan Analysis Results and Recommendations.

Use the **Pre-Scan Analysis Results and Recommendations** to address any identified network configuration issues before continuing the assessment.

Task

5/14/19, 11:08 AM

Review Pre-scan Analysis Results and Recommendations

The results from the pre-scan analysis will appear on the task details page.

Note: A 100% successful scan may not be possible in some cases due to network restrictions. Before opening ports or allowing protocols, please consult with your network and system administrator.

Below the Results Summary, refer to the **Recommendations** for specific suggestions for mitigating the issues that were identified.

Results Summary
Domains Found: 0
Computers in Active Directory: 0
Computers that can be scanned remotely (including non-A/D computers): 0
Computers in Active Directory that cannot be scanned remotely: 0
Users in Active Directory: 0

Overall: 2 Critical Issues, 0 recommendations
Active Directory: 1 Critical Issue, 0 recommendations
Internet: 0 Critical Issues, 0 recommendations
Network Computers: 1 Critical Issue, 0 recommendations
Push Deploy: 0 Critical Issues, 0 recommendations

Recommendations
[CRITICAL] A connection to Active Directory could not be established. Network scans of the Active Directory environment will be severely limited if the connection issue is not resolved prior to a complete scan. The following error was returned: The server is not operational.
Error details: User = administrator, DC = dc1
[CRITICAL] No computers were accessible via WMI or Remote Registry within the environment. This most likely points to a configuration issue or blocking by a local or remote firewall. For best results, please ensure that either WMI or Remote Registry is accessible remotely. Alternatively, the local data collector can be used to collect data on computers that are not remotely accessible.

Reference overview of critical issues and recommendations

Implement listed recommendations to ensure successful scans

Once you finish making any changes, click **Rerun Pre-scan Analysis** to check for any remaining issues.

Network Computers: 0 Critical issues, 0 recommendations

Push Deploy: 0 Critical issues, 0 recommendations

Recommendations

Click Mark Complete to initiate the Internal Network Scan.

Rerun Pre-scan Analysis

Adjust Scan Settings

✓

Mark Complete

When you have reviewed the pre-scan analysis and are finished making any recommended changes to the target network, click **Mark Complete**.

Step 7 — Collect CMMC Assessment Data

I. **Task** Complete External Port Use Worksheet.

Note: The **External Port Use Worksheet** will become available 1) once the **External Vulnerability Scan** is complete, and 2) one or more external ports are found to be open.

An attacker can exploit unnecessary open ports to gain access to the network. This worksheet details ports that were found to be open during the external vulnerability scan. Use this worksheet to document the business justification for each open port. Also indicate whether the port uses a secure protocol.

Port	Business Justification	Protocol Secure	Security Feature Documented
80/TCP		No	No
443/TCP		No	No

When you are finished, **Save**, and return to the To Do Item and click **Mark Complete**.

II. **Task** (*Automated*) Running the Automated Scan of the Internal Network.

The Compliance Manager server performs the **Internal Network Scan** on the target network. The Internal Scan begins automatically once you complete the pre-scan analysis and review the results.

Complete	5/10/19, 2:19 PM	Review Pre-scan Analysis Results and Recommendations
Complete	5/13/19, 10:27 AM	Complete External Port Use Worksheet
Task	5/13/19, 1:00 PM	Running Automated Scan of the Internal Network

Once the scan is complete, this To Do item will automatically be marked as complete.

**Running Automated Scan of the Internal Network**

A scan of your network has been started as part of the assessment process. Once the scan is complete, this To Do item will automatically be marked as complete.

Important: At least 1 computer must be successfully scanned in order for this To Do item to be automatically marked complete.

III. **Task** Running Local Scan of Remote Computers.

Once the Internal Network Scan is successfully completed, a scan of remote computers on the target network will automatically begin.

Complete	5/10/19, 2:10 PM	Review Pre-scan Analysis Results and Recommendations
Complete	5/13/19, 10:27 AM	Complete External Port Use Worksheet
Complete	5/13/19, 1:00 PM	Running Automated Scan of the Internal Network
Task	5/13/19, 1:26 PM	Running Local Scan of Remote Computers

This scan gathers more detailed data from individual endpoints on the target network.

**Running Local Scan of Remote Computers**

A scan of remote computers has been started as part of the assessment process. Once the scan is complete, this To Do item will automatically be marked as complete.

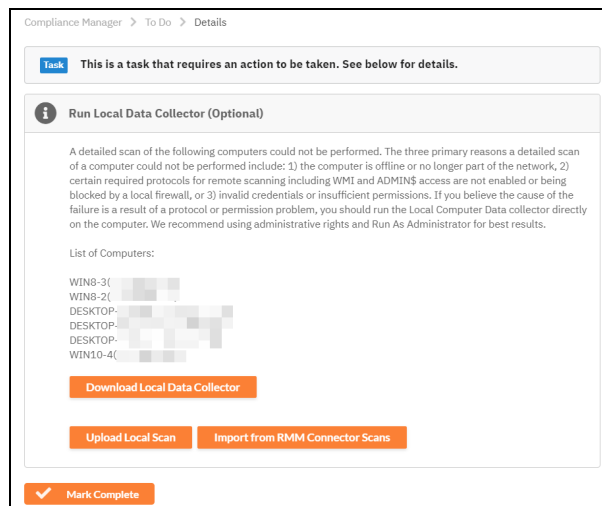
Important: At least 1 computer must be successfully scanned in order for this To Do item to be automatically marked complete.

- You will receive a separate To Do item if there is an error during the local scan of Remote Computers.
- You can then click **Go to Scan Settings** to change your scan configuration.
- You can also click **Initiate Rescan** once you fix any issues and wish to restart the scan.

IV. **Task** Run Local Data Collector (Optional).

In this task, you can perform manual scans on computers that could not be scanned automatically. You will also receive a list of known computers on the target network that could not be scanned. From this to do item, you can:

- A. Upload scans for computers that are connected to the network but cannot be scanned
- B. Upload scans for computers that are not available on the network being scanned, but that should be accounted for in the assessment process



Tip: You will also be notified if all computers are scanned successfully. You can then just click **Mark Complete** and move on with your assessment.

To perform the scan manually, first download the **Local Computer Data Collector** from <https://www.rapidfiretools.com/cm>. Run the Data Collector directly on the computer(s) and then upload the scan(s). Then click **Upload Local Scan**, and select the files or .zip files. When you are finished, click **Mark Complete**.

Note: You must **Mark Complete** this To Do task before you can proceed.

V. **Task** Complete Anti-virus Verification Worksheet.

Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. Use the **Anti-virus Verification Worksheet** to quickly determine if each endpoint on the network has anti-virus software installed.

To use the worksheet:

1. From the To Do list, click the **Go To Form** button to open the worksheet.

The screenshot shows the 'Anti-virus Verification Worksheet' in the Compliance Manager interface. The worksheet is titled '1.1 TEST' and contains a table with the following data:

Computer	IP Address	AV Detected	Detected Antivirus	Assessment
APV...	10.80...	Yes	Windows Defender	Verified Present
BACKUP...	10.80...	Yes	Windows Defender	Verified Present
DC...	10.80...	Yes	Windows Defender	Verified Present
DC...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present
DESKTOP...	10.80...	Yes	Windows Defender	Verified Present

2. The results of the scan for anti-virus software will appear in the worksheet for all PCs detected. Review the results:

- PCs detected with anti-virus will automatically be marked **Verified Present**.
- PCs detected without anti-virus will automatically be marked **Not Detected**.

Note: You can also manually change each response if needed. For example, you can mark a PC as **Verified Present** if you know the PC has anti-virus, but Compliance Manager did not detect it. Alternatively, you can mark the entry **Verified Not Present** if you know the PC does not have anti-virus installed.

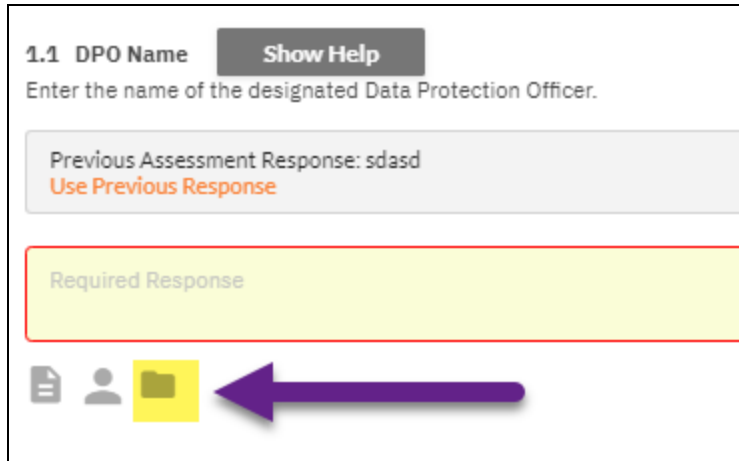
3. When are finished, **Save**, return to the To Do item and click **Mark Complete**.

Attach Supporting Documents

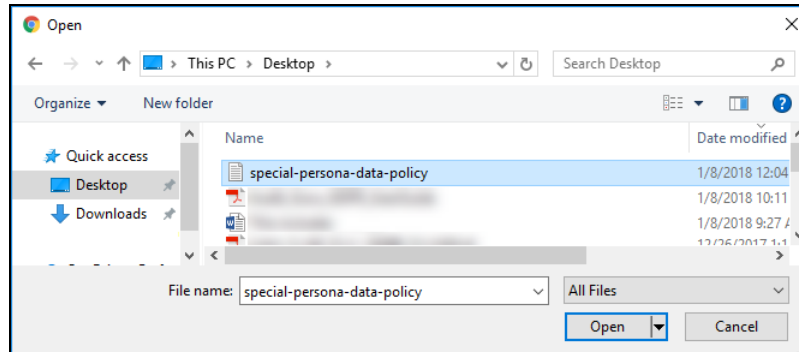
As evidence of compliance, you can add supporting documents that will be included as attachments when you generate assessment and compliance reports with

Compliance Manager. To attach a supporting document:

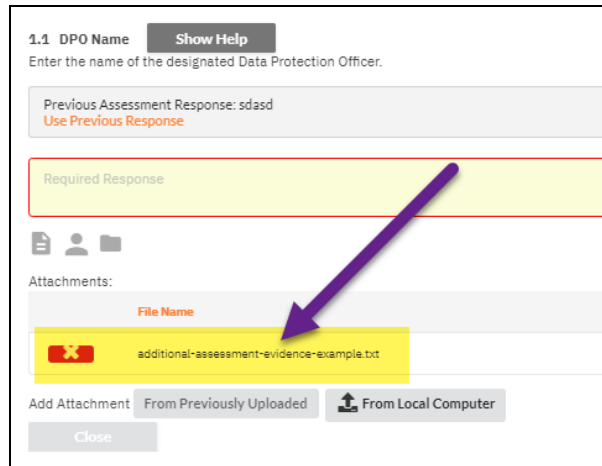
1. Click on the folder icon underneath the appropriate questionnaire field.



2. Choose whether to Add Attachment from **Previously Uploaded** or from your **Local Computer**.
3. Select the file you wish to upload and click Open. The selected file(s) will appear in the attachments queue.



- The file will be added to the assessment document as an attachment.




1.1 DPO Name [Show Help](#)


Enter the name of the designated Data Protection Officer.

Previous Assessment Response: sdsd
[Use Previous Response](#)

Required Response

Attachments:

File Name
 additional-assessment-evidence-example.txt

Add Attachment From Previously Uploaded  From Local Computer

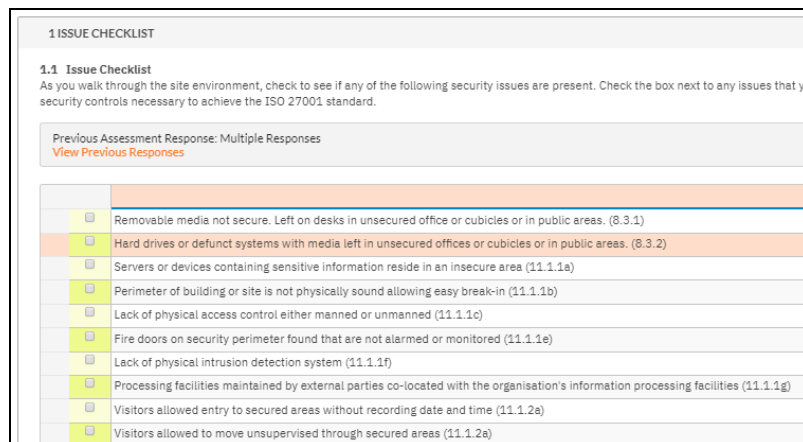
[Close](#)

Note: The attachment will appear in your supporting documents and reports that are generated at the end of the assessment process.

Select Multiple Fields

In worksheets that have tables with multiple fields, you can select several or all fields at once in order to enter responses more quickly. To select multiple fields:

- Click the left mouse button and hold on the first field you would like to include in the selection.



1 ISSUE CHECKLIST

1.1 Issue Checklist

As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Check the box next to any issues that you find that require security controls necessary to achieve the ISO 27001 standard.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)

2. While holding the left mouse button, drag and select your desired fields.

1 ISSUE CHECKLIST

1.1 Issue Checklist

As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you think require security controls necessary to achieve the ISO 27001 standard.

Previous Assessment Response: Multiple Responses

[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)
<input type="checkbox"/>	Lack of authentication mechanism to secure areas (11.1.2b)
<input type="checkbox"/>	Lack of physical or electronic audit trail for all access to secure areas (11.1.2c)
<input type="checkbox"/>	Employees, contractors, or external parties in secure area without visible identification (11.1.2d)

3. You can use this feature to copy and paste multiple responses at once. See ["Copy and Paste Responses"](#) below.

Copy and Paste Responses

Some worksheets allow you to copy and paste the responses you entered, much like a spreadsheet. This saves you time by allowing you to enter many responses at once. To do this:

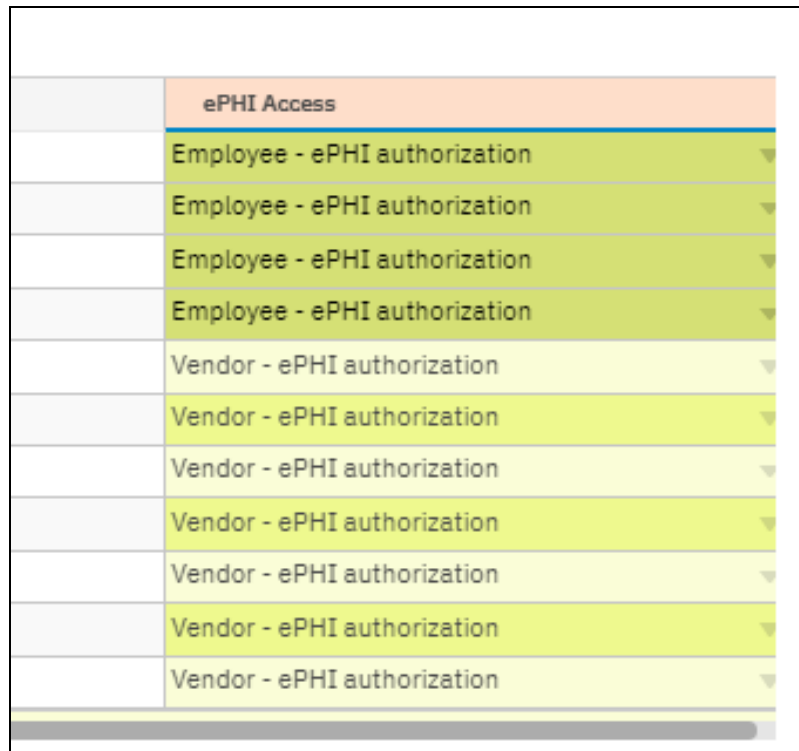
1. First answer one or more questions that require a response. Enter your response within the field.

Note: You can copy and paste both free-form and multiple choice entries.

(such as privileges) with the covered entity. For active employees and vendors, indicate if the user is

Last Login	ePHI Access
4/3/2018 4:16:37 AM	Employee - ePHI authorization
9/12/2018 6:25:29 AM	Employee - ePHI authorization
10/8/2018 9:14:33 AM	Employee - no ePHI authorization
1/16/2019 12:43:04 PM	Vendor - ePHI authorization
10/8/2018 9:29:47 AM	Vendor - no ePHI authorization
12/3/2018 9:20:19 AM	Former Employee
4/9/2018 4:17:06 AM	Employee - ePHI authorization

2. Use your mouse to drag and select multiple rows that contain the responses you wish to copy.



ePHI Access
Employee - ePHI authorization
Employee - ePHI authorization
Employee - ePHI authorization
Employee - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization
Vendor - ePHI authorization

3. On your keyboard, press **CTRL+C**.
4. Use your mouse to drag and select the rows you wish to paste the responses into.
5. On your keyboard, click **CTRL+V**. Your pasted responses will appear in the worksheet.

ty. For active employees and vendors, indicate if the user is

	ePHI Access
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization

Use this feature to save time completing worksheet responses that can be answered with the same answer.

VI. **Task** Complete User Access Review Worksheet.

The **User Access Review Worksheet** enables you to identify each user and to document their status: Employee, Third Party, Former Employee, Former Third Party, Service Account. You can also indicate whether each user has **Remote Access**.

Note: In addition to other scan procedures that identify Windows admin accounts, a user will also be marked as a "Privileged (Administrator) Account" if they are associated with any group or organizational unit that contains the word "admin."

To use the worksheet:

1. Click the **Go To Form** button to open the worksheet.

Compliance Manager > Assessments > InForm

User Access Review Worksheet

Select Assessment: Current Assessment

Search Topics

Hide # | Expand All | Collapse All | Download | Invite Others | Save | Save and Return | Return

1 TEST: .COM

1.1 User Access Review
The table below lists the users discovered on the network. For each user, specify the status. Then indicate whether the account has remote access.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

User Name	Display Name	Privileged (Administrator) Account	Last Login	Status	Has Remote Access?
		No	04-Jun-2019 3:47:12 PM	Former Employee	Yes
		No		Employee	Yes
		No		Employee	Yes
		Yes	29-May-2019 2:07:45 PM	Employee	Yes
		Yes	04-Jun-2019 10:19:51 AM	Employee	Yes

Compliance Manager > Assessments > InForm

User Access Review Worksheet

Select Assessment: Current Assessment

Search Topics

Hide # | Expand All | Collapse All | Download | Invite Others | Save | Save and Return | Return

1 TEST: .COM

1.1 User Access Review
The table below lists the users discovered on the network. For each user, specify the status. Then indicate whether the account has remote access and is current authorized to access CUI.

User Name	Display Name	Privileged (Administrator) Account	Last Login	Status	Has Remote Access?	Authorized?
			2020 7:02:08 PM			
			2020 8:22:55 AM			
			2019 10:12:29 AM			
			2020 7:34:54 AM			
			2020 2:55:24 PM			
			2019 10:14:12 AM			
			2019 10:13:48 AM			

0 required remaining

Save | Save and Return | Return

2. Assign each identified user the correct **Status**.
3. Indicate whether each user has **Remote Access**.
4. Indicate whether each user is **Authorized** to access the environment.
5. When are finished, **Save**, return to the To Do item and click **Mark Complete**.

VII. Task Complete Asset Inventory Worksheet.

Note: The Asset Inventory Worksheet will become available once the Internal Network Scan is complete.

The **Asset Inventory Worksheet** details the computer assets discovered on the network. Complete all of the required fields in the worksheet.

Compliance Manager > Assessments > InForm

Asset Inventory

Select Assessment: Current Assessment

Search Topics [Search]

Hide # | Expand All | Collapse All | Download

Save Save and Return

1 ASSET INVENTORY

1.1 Computer Asset Inventory

The table below details the computer assets discovered on the network. For each asset, specify the asset owner, acceptable use, environment, backup agent status, as well as device and sensitive information classification. For the Asset Owner, please enter the name of the person who is responsible for the information security of this asset. The owner does not need to be the actual user of the system. In the Acceptable Use column, enter a short description of the primary acceptable use for this system (i.e., "user workstation").

Device Name	Device Type	Device Type	Operating System	System Description	Asset Owner	Acceptable Use	Environment	Has Backup Agent	Device Classification	Sensitive Information Classification
APP0	Server	fe80	Windows Server 2016 Standard							
BACKUP0	Server	fe80	Windows Server 2016 Standard							
DC0	Server	fe80	Windows Server 2016 Standard							
DC0	Server	fe80	Windows Server 2016 Standard							
DESKTOP-09	Workstation	fe80	Windows 10 Pro							
DESKTOP-19	Workstation	fe80	Windows 10 Enterprise							
DESKTOP-35	Workstation	fe80	Windows 10 Enterprise							
DESKTOP-4P	Workstation	fe80	Windows 10 Pro							
DESKTOP-53	Workstation	fe80	Windows 10 Enterprise							

VIII. Task Complete Application Inventory Worksheet.

This worksheet details the applications discovered on the network. For each application, specify whether the app is necessary for the organization and its operation; unnecessary apps should be removed from the environment.

Note: The apps in this worksheet are discovered during the network scan — and you might find that certain apps are redundant or not authorized by the organization. In this case, they can be removed from the network.

Compliance Manager > Assessments > InForm

Application Inventory

Select Assessment: Current Assessment

English (US)

Search Topics [Search]

Hide # | Expand All | Collapse All | Download

Invite Others Save Save and Return Return

1 APPLICATION INVENTORY

1.1 Application Inventory

The table below details the applications discovered on the network. For each application, specify if the application is "Necessary".

Application	Number of Computers	List of Computers	Is Necessary?
Google Chrome	7		Yes
Intel(R) Processor Graphics	2		Yes
Java 8 Update 191	2		Yes
Java 8 Update 201	1		Yes
Java 8 Update 241	1		Yes
Jenkins 2.204.2	1		Yes
jNestMap	1		Yes

0 required remaining

Save Save and Return Return

IX. Task Complete External Information System Worksheet.

This worksheet is used to document external information systems used by your organization. Add entries for each external information system along with a description, purpose for using the system, name of the business owner of the system, along with its criticality. Examples of external information systems include Salesforce, QuickBooks Online, and Office 365.

The purpose of this worksheet is to inventory systems in use at the organization, but that are largely outside of (external to) that organization's control and/or ownership. This can allow the organization to manage the risk posed by using external systems. Specifically, you must:

- Identity each external info system
- Determine the business owner and business purpose of that system
- Establish the business priority (criticality) of that system

The screenshot shows the 'External Information System Worksheet' interface. At the top, there's a breadcrumb trail: 'Compliance Manager > Assessments > Inform'. Below this, the title 'External Information System Worksheet' is displayed. To the right, there are dropdowns for 'English (US)' and 'Select Assessment' (set to 'Current Assessment'). A search bar with 'Search Topics' and a 'Search' button is present. Below the search bar, there are buttons for 'Hide # | Expand All | Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The main content area is titled '1 EXTERNAL INFORMATION SYSTEMS' and contains a section '1.1 External Information Systems' with a descriptive paragraph. Below the text is a table with five columns: 'Name', 'Description', 'Purpose', 'Business Owner', and 'Criticality'. The table is currently empty. At the bottom right of the table area, there are 'Save', 'Save and Return', and 'Return' buttons. A 'Jump To Top' link is at the bottom left.

Enter each information system one line at a time. Complete all relevant fields for each entry.

This screenshot shows the same interface as the previous one, but with an example entry added to the table. The table has three rows: a header row with columns 'Name', 'Description', and 'Purpose', and two data rows. The first data row contains 'Gmail' in the 'Name' column, 'Email system' in the 'Description' column, and 'Office communication' in the 'Purpose' column. The second data row is empty. The 'Save', 'Save and Return', and 'Return' buttons are still visible at the bottom right.

X. **Task** Select Level of CMMC Assessment.

In this step, choose whether you wish to perform a **Level 1**, **Level 2**, or **Level 3** CMMC Assessment.

Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

Select Level of CMMC Assessment

Select Level of the CMMC Assessment that you want to perform.

The Cybersecurity Maturity Model (CMM) and its control domains have “Levels” of IT security controls that can be implemented to secure an information system and access to CUI.

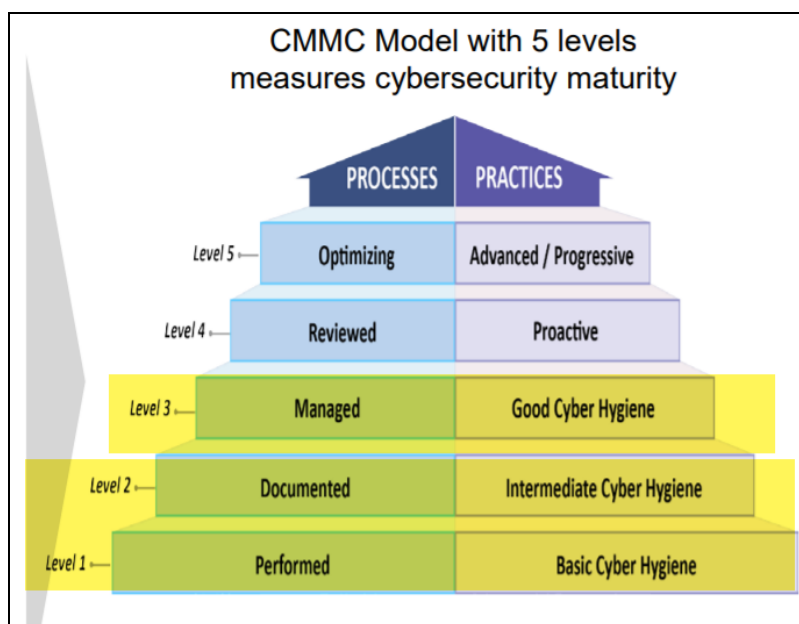
Compliance Manager enables an assessor to perform a CMMC assessment based on CMMC control levels 1, 2 and 3.

Select the level of the CMMC Assessment you want to perform.

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

☒ **Mark Complete**

CMMC has multiple “Levels” of IT security controls that can be implemented to secure the IT environment. **Level 1, Level 2, Level 3** represent the first two levels of the CMMC assessment.



Note: To learn more about the CMMC model and its associated levels, visit <https://www.acq.osd.mil/cmmc/>.

Which CMMC Level Should I Choose?

- The **Level 1** assessment presents fewer worksheets for the auditor to complete. In addition, the CMMC worksheets will be simplified and contain fewer questions. Use this level if you want to perform a relatively quick "Basic Cyber Hygiene" check as per the CMMC framework.
- The **Level 2** assessment presents several additional worksheets to complete. Likewise, the CMMC worksheets will contain added sections and questions. Use this level if you want to perform an "Intermediate Cyber Hygiene" check as per the CMMC framework. Once you complete a Level 2 assessment, you will have a wealth of documentation to support your Level 2 compliance.

The **Level 3** allows you to perform a "Good Cyber Hygiene" check as per the CMMC framework. Once you complete a Level 3 assessment, you will have a wealth of documentation to support your Level 3 compliance.

Change Assessment Level

During your assessment, you may decide to change CMMC assessment levels. To do this:

1. Return to the **Select CMMC Level** to do item.
2. Click Re-run and select your desired assessment level. Confirm that you wish to regenerate the worksheet To Do items.

Compliance Manager > To Do > Details

Complete This issue/task has been marked complete.

i **Select Level of CMMC Assessment**

Select Level of the CMMC Assessment that you want to perform.

The Cybersecurity Maturity Model (CMM) and its control domains have “Levels” of IT security controls that can be implemented to secure an information system and access to CUI.

Compliance Manager enables an assessor to perform a CMMC assessment based on CMMC control levels 1, 2 and 3.

Select the level of the CMMC Assessment you want to perform.

Level 1 Level 2 Level 3

✓ Completed **Re-run** ←

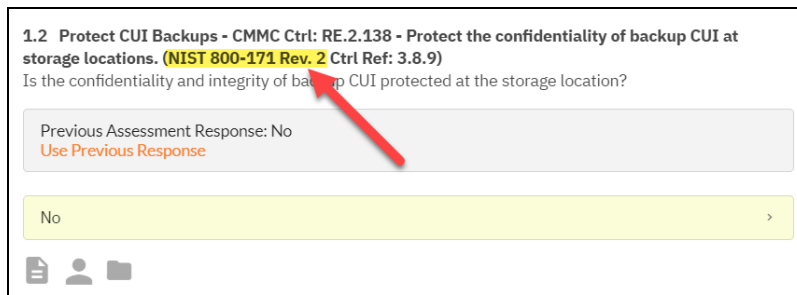
Your To Do list will be updated with the worksheets for the selected level.

Note: Your saved responses will be available to re-use in the regenerated worksheets.

Step 8A — Complete Level 1 CMMC Worksheets

Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.



1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)

Is the confidentiality and integrity of backup CUI protected at the storage location?

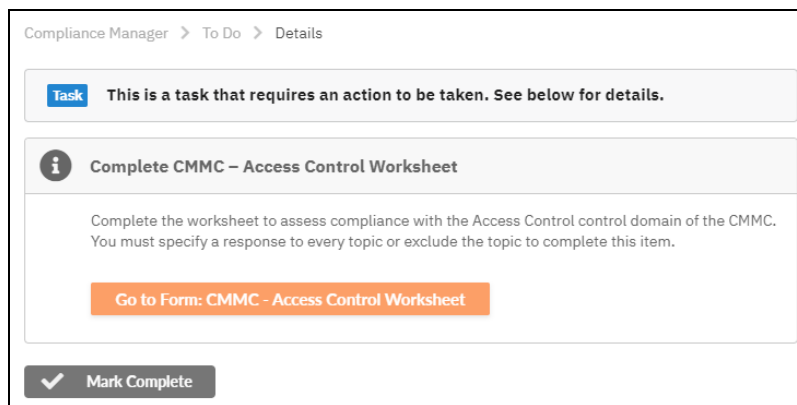
Previous Assessment Response: No
[Use Previous Response](#)

No >

Icons: Document, User, Folder

I. **Task** Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.



Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

Complete CMMC - Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

☒ Mark Complete

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems

- Utilization of the principle of least privilege for user accounts and their access to sensitive data

The screenshot shows the 'CMMC Access Control Worksheet' in the Compliance Manager application. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and a 'Select Assessment' dropdown. Below this, there are buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content is divided into sections for different CMMC domains, with the first section being '1. C001 - ESTABLISH SYSTEM ACCESS REQUIREMENTS (REQUIRED REMAINING)'. It lists specific requirements like '1.1 Limit system access' and '1.2 Privacy and Security Notices', each with a description and a 'Show Guidance' link. At the bottom, there's a status bar indicating '22 required remaining' and buttons for 'Save', 'Save and Return', and 'Return'.

II. **Task** Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the Compliance Manager interface. The card has a title 'Complete CMMC – Identification and Authentication Worksheet' and a description: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Identification and Authentication Worksheet'. At the bottom of the card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Initiate Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 C015- GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)' and three numbered sections: 1.1 User Accounts, 1.2 Identify Users, and 1.3 Password Complexity. Each section contains a question, a 'Show Guidance' link, and a yellow input field. At the bottom, it says '11 required remaining' with 'Save', 'Save and Return', and 'Return' buttons.

III. **Task** Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details in the 'Compliance Manager' interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A blue 'Task' icon is followed by the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Media Protection Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' An orange button labeled 'Go to Form: CMMC - Media Protection Worksheet' is present. At the bottom is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main area is titled 'CMMC Media Protection Worksheet' and includes a search bar, a 'Select Assessment' dropdown (set to 'Current Assessment'), and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a message states: 'Complete the following worksheet regarding the compliance with the CMMC – Media Protection (MP) control domain. This worksheet should be completed by an Internal Auditor.' A section titled '1 C023 - PROTECT AND CONTROL MEDIA IS REQUIRED REMAINING' contains three numbered items: 1.1, 1.2, and 1.3, each with a description and a 'Show Guidance' link. Each item has a corresponding form field with a yellow background and a red border. At the bottom, it says '8 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

IV. **Task** Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC – Physical Protection Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of this section is an orange button that says 'Go to Form: CMMC - Physical Protection Worksheet'. At the very bottom of the card is a grey button with a checkmark icon that says 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Physical Protection Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a message states: 'Complete the following worksheet regarding the compliance with the CMMC - Physical Protection (PE) control domain. This worksheet should be completed by an Internal Auditor'. The worksheet content includes: '1 CO28 - LIMIT PHYSICAL ACCESS (6 REQUIRED REMAINING)', '1.1 Control Physical Access - CMMC Ctrl: PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.3) Does the company limit physical access to information systems, equipment, and system operating environments to authorized individuals? (Show Guidance)', and '1.2 Visitor Access Monitoring - CMMC Ctrl: PE.1.132 - Escort visitors and monitor visitor activity. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.3) Does the company escort visitors and monitor visitor activity in locations where information systems are located or to use? (Show Guidance)'. At the bottom, it says '1.3 Access Audit Logs - CMMC Ctrl: PE.1.133 - Maintain audit logs of physical access. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.4) 6 required remaining' with 'Save', 'Save and Return', and 'Return' buttons.

V. **Task** Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – System and Communications Protection Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button that says 'Go to Form: CMMC - Systems and Communication Protection Worksheet'. Below the card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main area displays the 'CMMC System and Communications Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions: 'Complete the following worksheet regarding the compliance with the controls contain within the CMMC - System and Communications Protection (SC) control domain. This worksheet should be completed by an Internal Auditor.' It lists two tasks: '1. CO38 - DEFINE SECURITY REQUIREMENTS FOR SYSTEMS AND COMMUNICATIONS (15 REQUIRED REMAINING)' and '1.1 Collaborative Computing Devices - CMMC Ctrl: SC.2.178 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (NIST 800-571 Rev. 2 Ctrl Ref: 3.13.52)'. Each task has a 'Show Guidance' link and a yellow input field. At the bottom, it says '19 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

VI. **Task** Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – System and Information Integrity Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is an orange button that says 'Go to Form: CMMC - System and Information Integrity Worksheet'. At the bottom is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans for Federal Information Systems," page 19, section 3, "Plan

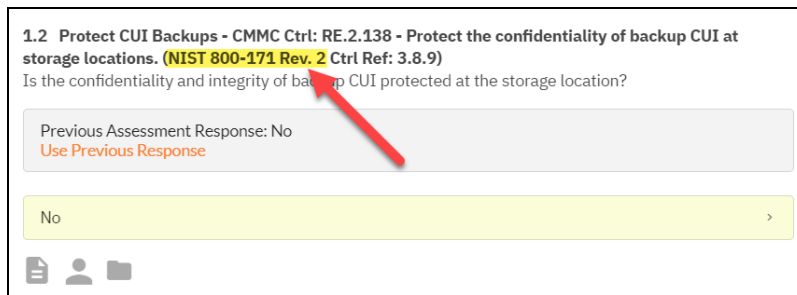
Development." This document is currently available at:
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

The screenshot displays the 'CMMC Demo Site 2' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Settings, and Audit Log. The main content area is titled 'CMMC System and Information Integrity Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Search', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below these is a section for '1 INFORMATION SYSTEM NAME AND TITLE (3 REQUIRED REMAINING)'. Under this, there are two sub-sections: '1.1 System Name' with instructions to 'State the name of the system in the field below. Spell out acronyms.' and '1.2 System Categorization' with instructions to 'Enter the System Categorization in the field below.'. Each sub-section has a 'Required Response' text input field. At the bottom left, it says '13 required remaining'. At the bottom right, there are 'Save', 'Save and Return', and 'Return' buttons.

Step 8B — Complete Level 2 CMMC Worksheets

Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.



1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)

Is the confidentiality and integrity of backup CUI protected at the storage location?

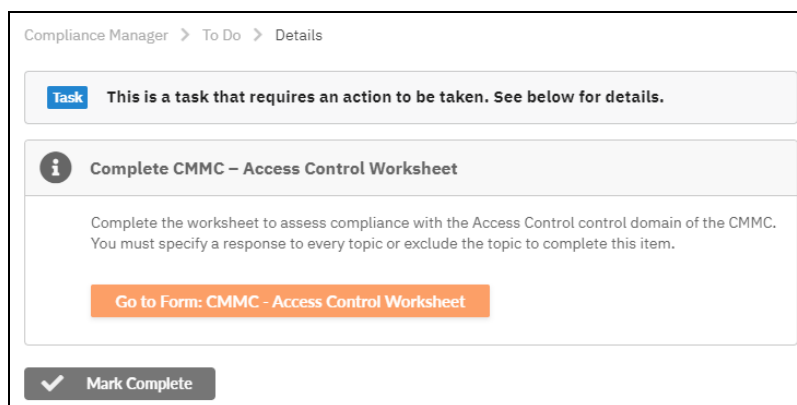
Previous Assessment Response: No
[Use Previous Response](#)

No >

Icons: Document, User, Folder

I. **Task** Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.



Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

Complete CMMC – Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

☒ Mark Complete

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems

- Utilization of the principle of least privilege for user accounts and their access to sensitive data

The screenshot shows the 'CMMC Access Control Worksheet' within the 'Acme CMMC Project'. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays a search bar, a 'Select Assessment' dropdown, and a 'Current Assessment' dropdown. Below these, there are buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content is titled 'Complete the following worksheet regarding the compliance with the CMMC - Access Control (AC) control domain. This worksheet should be completed by an Internal Auditor.' It lists three sections: 1. CO01 - ESTABLISH SYSTEM ACCESS REQUIREMENTS (REQUIRED REMAINING), 1.1 Limit system access - CMMC CUI: AC.1.001 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and 1.2 Privacy and Security Notices - CMMC CUI: AC.2.000 - Provide privacy and security notices consistent with applicable CUI rules. Each section has a 'Show Guidance' link and a text input field. At the bottom, it shows '22 required remaining' and buttons for 'Save', 'Save and Return', and 'Return'.

II. **Task** Complete CMMC Asset Management Worksheet

Complete the **CMMC Asset Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. The sidebar includes navigation options like Home, Compliance Manager, To Do, Assessments, Settings, and Audit Log. The main content area displays a 'Task' section with the title 'Complete CMMC - Asset Management Worksheet'. Below the title, there is a description: 'Complete the worksheet to assess compliance with the Assessment Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this form.' There is a 'Go to Form: CMMC - Asset Management Worksheet' button and a 'Mark Complete' button. The URL at the bottom is 'http://users.user-central-staging.com/CMDC-Demo-Site-2/audit-gui/assessments/forms/C01NQ8B8C3N8C8NY8N2V0K0088comz09K87g0D98'.

Specifically, this worksheet asks you to examine processes and procedures in place in order to manage "controlled unclassified information" (CUI).

The screenshot shows the 'CMMC Asset Management Worksheet' in the Compliance Manager application. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area has a breadcrumb trail: Compliance Manager > Assessments > InfoForm. Below this is the title 'CMMC Asset Management Worksheet' and a 'Select Assessment' dropdown set to 'Current Assessment'. A search bar is present. Below the search bar are buttons: 'Hide # | Expand All | Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. A message states: 'Complete the following worksheet regarding the compliance with the CMMC - Asset Management (AM) control domain. This worksheet should be completed by an Internal Auditor'. A progress bar shows '1 CROS-IDENTIFY AND DOCUMENT ASSETS (15 REQUIRED REMAINING)'. A specific task is listed: '5.1 CUI Handling - CMMC CSE AM.3.036 - Define procedures for the handling of CUI data. Does the company have procedures for the handling of CUI data consistent with DoD instructions? (Reference publication: DoD 5200.48 Controlled Unclassified Information) (Show Guidance)'. Below this is a large yellow text input area. At the bottom, there is a 'Jump To Top' link and a status bar showing '1 required remaining' with 'Save', 'Save and Return', and 'Return' buttons.

III. **Task** Complete CMMC Audit and Accountability Worksheet

Complete the **CMMC Audit and Accountability Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Audit and Accountability Worksheet' with an information icon. The description reads: 'Complete the worksheet to assess compliance with the Audit and Accountability control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is an orange button labeled 'Go to Form: CMMC - Audit and Accountability Worksheet'. At the bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Event logging of individual system users and their actions
- Audit log retention
- Audit log review

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Audit and Accountability Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Invites Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for the CMMC – Audit and Accountability (AU) control domain. It lists two tasks: '1.007 - DEFINE AUDIT REQUIREMENTS (3 REQUIRED REMAINING)' and '1.1 Event Logging - CMMC Ctrl: AU.2.045 - Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. (NIST 800-571 Rev. 2 Ctrl Ref 3.3.2)'. Each task has a 'Show Guidance' link and a yellow input field. At the bottom, it says '11 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

IV. **Task** Complete CMMC Awareness and Training Worksheet

Complete the **CMMC Awareness and Training Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details for 'Complete CMMC - Awareness and Training Worksheet'. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A 'Task' box states: 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC - Awareness and Training Worksheet'. The text inside says: 'Complete the worksheet to assess compliance with the Awareness and Training control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button that says 'Go to Form: CMMC - Awareness and Training Worksheet'. At the bottom is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- The status of security awareness training at the organization
- The status of role-based security awareness training at the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Awareness and Training Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for the CMMC – Awareness and Training (AT) control domain. It lists two tasks: 1.1 'CONDUCT SECURITY AWARENESS ACTIVITIES (2 REQUIRED REMAINING)' and 1.2 'Insider Threat Awareness Training - CMMC Ctrl: AT.3.058'. Each task has a description, a 'Show Guidance' link, and a large yellow input field. At the bottom, it says '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

V. **Task** Complete CMMC Configuration Management Worksheet

Complete the **CMMC Configuration Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' card with the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information card titled 'Complete CMMC – Configuration Management Worksheet' with an 'i' icon. The card contains the instruction: 'Complete the worksheet to assess compliance with the Configuration Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the instruction is an orange button labeled 'Go to Form: CMMC - Configuration Management Worksheet'. At the bottom of the details view is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Establish configuration baselines: Ensure principle of least functionality is employed; restrictions on user-installed software.
- Configuration change management: Ensure organization analyzes security configuration changes and establishes and enforces baseline security settings.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Configuration Management Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Search', 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Configuration Management (CM) control domain. This worksheet should be completed by an Internal Auditor.' It lists two tasks: '1 CO13 - ESTABLISH CONFIGURATION BASELINES (2 REQUIRED REMAINING)' and '1.1 Baseline Configuration - CMMC Ctrl: CM.2.061 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.1)'. Below each task is a yellow input field with a dropdown arrow. At the bottom, it says '9 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

VI. **Task** Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' header and a message: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC – Identification and Authentication Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of this section is an orange button that says 'Go to Form: CMMC - Identification and Authentication Worksheet'. At the very bottom of the card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot shows the 'Acme CMMC Project' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Limit Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header 'Complete the following worksheet regarding the compliance with the CMMC - Identification and Authentication (IA) control domain. This worksheet should be completed by an Internal Auditor.' and a section '1 C015- GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)'. Below this are three numbered tasks: 1.1 User Accounts, 1.2 Identify Users, and 1.3 Password Complexity. Each task has a description, a 'Show Guidance' link, and a yellow input field with a dropdown arrow. At the bottom, there are 'Save', 'Save and Return', and 'Return' buttons.

VII. **Task** Complete CMMC Incident Response Worksheet

Complete the **CMMC Incident Response Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details in the 'Compliance Manager' interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A blue 'Task' label is followed by the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Incident Response Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Incident Response control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Incident Response Worksheet'. At the bottom is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Detail the organization's plan for handling a security incident, including planning, responding, reporting, analyzing, and testing.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Incident Response Worksheet' and includes a search bar and buttons for 'Initiate Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header 'Complete the following worksheet regarding the compliance with the CMMC - Incident Response (IR) control domain. This worksheet should be completed by an Internal Auditor.' followed by two sections: '1 CSD16- INCIDENT PLAN/RESPONSE (3 REQUIRED REMAINING)' and '2 CD17- DETECT AND REPORT EVENTS (2 REQUIRED REMAINING)'. Each section contains a sub-section with a title and a description, followed by a yellow input field and a 'Show Guidance' link. At the bottom, it indicates '7 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

VIII. **Task** Complete CMMC Maintenance Worksheet

Complete the **CMMC Maintenance Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' icon and text: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Maintenance Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Maintenance control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of this section is an orange button labeled 'Go to Form: CMMC - Maintenance Worksheet'. At the very bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Management of IT maintenance tools and management of IT personnel
- Multifactor authentication for remote access maintenance tools

The screenshot shows the 'CMMC Maintenance Worksheet' form within the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area has a breadcrumb trail 'Compliance Manager > Assessments > InfoForm' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below the header, there are buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', '14 Invite Others', 'Save', 'Save and Return', and 'Return'. A message states: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Maintenance (MA) control domain. This worksheet should be completed by an Internal Auditor.' A status bar indicates '1 C021 - MANAGE MAINTENANCE IS REQUIRED REMAINING'. The form contains three sections: 1.1 Maintenance Tools - CMMC Ctrl: MA.2.111 - Perform maintenance on organizational systems, 1.2 Controlled Maintenance - CMMC Ctrl: MA.2.112 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance, and 1.3 Nonlocal Maintenance - CMMC Ctrl: MA.2.113 - Require multifactor authentication to establish nonlocal maintenance sessions. Each section has a 'Show Guidance' link and a text input field. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

IX. **Task** Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' icon and the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Media Protection Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is an orange button labeled 'Go to Form: CMMC - Media Protection Worksheet'. At the bottom of the card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'CMMC Media Protection Worksheet' in the Compliance Manager application. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a message states: 'Complete the following worksheet regarding the compliance with the CMMC – Media Protection (MP) control domain. This worksheet should be completed by an Internal Auditor.' A progress indicator shows '1 CO23 - PROTECT AND CONTROL MEDIA IS REQUIRED REMAINING'. The worksheet contains three sections: 1.1 'Protect and Control - CMMC Ctrl: MP.2.120 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.1)', 1.2 'Protect and Control - CMMC Ctrl: MP.2.120 - Limit access to CUI on system media to authorized users, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.2)', and 1.3 'Protect and Control - CMMC Ctrl: MP.2.121 - Control the use of removable media on system components, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.7)'. Each section has a 'Show Guidance' link and a large yellow input field. At the bottom, it says '8 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

X. **Task** Complete CMMC Personnel Security Worksheet

Complete the **CMMC Personnel Security Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card in the Compliance Manager 'To Do' section. The card title is 'Complete CMMC – Personnel Security Worksheet'. Below the title, it says: 'Complete the worksheet to assess compliance with the Personnel Security control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is an orange button labeled 'Go to Form: CMMC - Personnel Security Worksheet'. At the bottom of the card, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Procedures to screen individuals before employment and access to sensitive data
- Procedures to restrict employee data access after they leave the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Personnel Security Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', '14 Items Other', 'Save', 'Save and Return', and 'Return'. Below this is a detailed instruction: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Personnel Security (PS) control domain. This worksheet should be completed by an Internal Auditor.' The worksheet contains two sections: '1 CO26 - SCREEN PERSONNEL (1 REQUIRED REMAINING)' and '2 CO27 - PROTECT CUI DURING PERSONNEL ACTIONS (1 REQUIRED REMAINING)'. Each section has a sub-item with a description and a 'Show Guidance' link. At the bottom, it indicates '2 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XI. **Task** Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Physical Protection Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of this section is an orange button labeled 'Go to Form: CMMC - Physical Protection Worksheet'. At the very bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot displays the 'Acme CMMC Project' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Physical Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 CO28 - LIMIT PHYSICAL ACCESS (6 REQUIRED REMAINING)' and instructions: 'Complete the following worksheet regarding the compliance with the CMMC - Physical Protection (PE) control domain. This worksheet should be completed by an Internal Auditor'. It lists three sections: 1.1 Control Physical Access - CMMC Ctrl: PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.3) [Show Guidance]; 1.2 Visitor Access Monitoring - CMMC Ctrl: PE.1.132 - Escort visitors and monitor visitor activity. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.3) [Show Guidance]; and 1.3 Access Audit Logs - CMMC Ctrl: PE.1.133 - Maintain audit logs of physical access. (NIST 800-571 Rev. 2 Ctrl Ref: 3.10.4). Each section has a yellow input field and a 'Show Guidance' link. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XII. **Task** Complete CMMC Recovery Worksheet

Complete the CMMC Recovery worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details page in the 'Compliance Manager > To Do > Details' view. It features a 'Task' header with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Recovery Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Recovery control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button labeled 'Go to Form: CMMC - Recovery Worksheet' is present. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Regular performance and testing of data backups
- Protection of CUI data after backup

The screenshot shows the 'Acme CMMC Project' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Recovery Worksheet' and includes a search bar, a 'Select Assessment' dropdown (set to 'Current Assessment'), and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 C029 - MANAGED BACKUPS (3 REQUIRED REMAINING)' and three numbered tasks: 1.1 'Regularly Perform and Test Data Backups - CMMC Ctl: RE.3.137 - Regularly perform and test data backups.', 1.2 'Protect CUI Backups - CMMC Ctl: RE.3.138 - Protect the confidentiality of backup CUI at storage locations.', and 1.3 'Perform Comprehensive Backups - CMMC Ctl: RE.3.139 - Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.' Each task has a yellow progress bar and a 'Show Guidance' link. At the bottom, it says '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XIII. **Task** Complete CMMC Risk Management Worksheet

Complete the **CMMC Risk Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' icon and text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Risk Management Worksheet'. The main text reads: 'Complete the worksheet to assess compliance with the Risk Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button that says 'Go to Form: CMMC - Risk Management Worksheet'. Below the card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Risk and vulnerability assessment
- Vulnerability scanning
- Vulnerability remediation

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Risk Management Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', '14 Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, there is a section for '1 CO31 - IDENTIFY AND EVALUATE RISK (3 REQUIRED REMAINING)'. It contains two sub-sections: '1.1 Risk Assessment - CMMC CUI: RM.2.541 - Periodically assess the risk to organizational operations...' and '1.2 Vulnerability Scanning - CMMC CUI: RM.2.542 - Scan for vulnerabilities in organizational systems...'. Each sub-section has a text input field and a 'Show Guidance' link. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XIV. **Task** Complete CMMC Security Assessment Worksheet

Complete the CMMC Security Assessment worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do (highlighted), Assessments, Settings, and Audit Log. The main content area is titled 'CMMC Demo Site 2' and includes a breadcrumb trail 'Compliance Manager > To Do > Details'. Below this, there is a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' and an information icon. Below the information icon is a section titled 'Complete CMMC - Security Assessment Worksheet' with the text 'Complete the worksheet to assess compliance with the Security Assessment control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' and a button 'Go to Form: CMMC - Security Assessment Worksheet'. At the bottom, there is a 'Mark Complete' button.

Specifically, this worksheet asks you to examine:

- Existence of a system security plan
- Assessment of the security plan
- Plans of action against vulnerabilities

The screenshot shows the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Security Assessment Worksheet'. It includes a search bar, a 'Select Assessment' dropdown (set to 'Current Assessment'), and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Security Assessment (CA) control domain. This worksheet should be completed by an Internal Auditor.' It lists two sections: '1 C034 - DEVELOP AND MANAGE A SYSTEM SECURITY PLAN (1 REQUIRED REMAINING)' and '2 C035 - DEFINE AND MANAGE CONTROLS (3 REQUIRED REMAINING)'. Each section contains specific requirements and a 'Show Guidance' link. At the bottom, it indicates '5 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XV. **Task** Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task Details' view in the Compliance Manager interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A blue 'Task' icon is followed by the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon (i) followed by the title 'Complete CMMC – System and Communications Protection Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the task card is an orange button that says 'Go to Form: CMMC - Systems and Communication Protection Worksheet'. Below the task card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The 'Forms' option is selected. The main content area is titled 'CMMC System and Communications Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown (set to 'Current Assessment'), and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, there is a section for '1 CO38 - DEFINE SECURITY REQUIREMENTS FOR SYSTEMS AND COMMUNICATIONS (15 REQUIRED REMAINING)'. It lists two items: '1.1 Collaborative Computing Devices - CMMC Ctrl: SC.2.178 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (NIST 800-571 Rev. 2 Ctrl Ref: 3.13.52)' and '1.2 Session Encryption - CMMC Ctrl: SC.2.179 - Use encrypted sessions for the management of network devices.' Each item has a 'Show Guidance' link and a yellow input field. At the bottom, it says '19 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XVI. **Task** Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' section in the Compliance Manager interface. It has a breadcrumb trail: 'Compliance Manager > To Do > Details'. Below this is a 'Task' box with the text: 'This is a task that requires an action to be taken. See below for details.' Below the task box is an information box titled 'Complete CMMC – System and Information Integrity Worksheet'. It contains the text: 'Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below this text is an orange button that says 'Go to Form: CMMC - System and Information Integrity Worksheet'. At the bottom of the information box is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans for Federal Information Systems," page 19, section 3, "Plan

Development." This document is currently available at:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

XVII. **Task** Complete NIST 800-171 Scoring Supplement Worksheet (Optional)

In summer 2020, the Department of Defense (DoD) introduced a self-assessment methodology to allow contractors to achieve interim certification before the eventual implementation of the complete CMMC program.

The optional **NIST 800-171 Scoring Supplement** allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in the form of a DoD Assessment Score.

This worksheet should be completed by an Internal Auditor.

The NIST 800-171 Scoring Supplement contains and cross-references the CMMC Control Domains that are relevant to the NIST 800-171 Security Requirement.

The screenshot displays the 'Acme CMMS Project' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'NIST 800 171 Scoring Supplement' and includes a search bar, a 'Select Assessment' dropdown (set to 'Current Assessment'), and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below these are 'Previous Page' and 'Next Page' buttons, with 'Page 1 of 2' indicated. The worksheet content includes a header '1 ACCESS CONTROL (AC) (8 REQUIRED REMAINING)' and two sections: '1.1 Wireless Access and Encryption - CHMRC Ctrl: AC.3.013 - Protect wireless access using authentication and encryption. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.37)' and '1.2 Protect Remote Access - CHMRC Ctrl: AC.3.014 - Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.53)'. Each section has a 'Show Guidance' link and a large yellow text input field. At the bottom, there are 'Previous Page', 'Next Page', 'Page 1 of 2', 'Save', 'Save and Return', and 'Return' buttons.

Note: Issues generated as a result of your responses to the NIST 800-171 Scoring Supplement Worksheet **do not** currently appear in the Compensating Controls Worksheet. Update your responses in the NIST 800-171 worksheet itself to indicate any mitigation measures taken to resolve issues identified. Return to the Worksheet To Do item, click the "Modify" button, and modify the worksheet responses to reflect the remediation actions undertaken.

Complete the Scoring Supplement to access the following compliance reports at the end of your assessment:

- CUI Plan of Action and Milestones Report
- CUI System Security Plan
- NIST 800 171 Scoring Supplement Worksheet
- NIST SP 800 171 DoD Assessment Score Report

Step 8C — Complete Level 3 CMMC Worksheets

Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.

1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)

Is the confidentiality and integrity of backup CUI protected at the storage location?

Previous Assessment Response: No
[Use Previous Response](#)

No >

Icons: Document, User, Folder

I. **Task** Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

Complete CMMC – Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

☒ Mark Complete

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems

- Utilization of the principle of least privilege for user accounts and their access to sensitive data

The screenshot shows the 'CMMC Access Control Worksheet' within the 'Acme CMMC Project'. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title and a search bar. Below the title, there are buttons for 'Hide #', 'Expand All', 'Collapse All', and 'Download'. A 'Select Assessment' dropdown is set to 'Current Assessment'. The worksheet content is divided into sections for different CMMC domains, with a 'REQUIRED REMAINING' status indicator. The first section is '1.001 - ESTABLISH SYSTEM ACCESS REQUIREMENTS', which includes a sub-section '1.1 Limit system access - CMMC Ctl: AC.1.001 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) (NIST 800-171 Rev. 2 Ctl Ref: 3.3.1)'. The second section is '1.2 Privacy and Security Notices - CMMC Ctl: AC.2.005 - Provide privacy and security notices consistent with applicable CUI rules. (NIST 800-171 Rev. 2 Ctl Ref: 3.3.9)'. The third section is '1.3 Limit Portable Storage Device Use - CMMC Ctl: AC.2.006 - Limit use of portable storage devices on external systems. (NIST 800-171 Rev. 2 Ctl Ref: 3.3.23)'. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return'.

II. **Task** Complete CMMC Audit and Accountability Worksheet

Complete the **CMMC Audit and Accountability Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and a message: 'This is a task that requires an action to be taken. See below for details.' Below this, there is an information icon and the title 'Complete CMMC - Audit and Accountability Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Audit and Accountability control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card, there is an orange button labeled 'Go to Form: CMMC - Audit and Accountability Worksheet'. Below the card, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Event logging of individual system users and their actions
- Audit log retention
- Audit log review

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Audit and Accountability Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Invites Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for organizational compliance, followed by two sections: '1. CO07 - DEFINE AUDIT REQUIREMENTS (3 REQUIRED REMAINING)' and '1.1 Event Logging - CMMC Ctrl: AU.2.045 - Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. (NIST 800-571 Rev. 2 Ctrl Ref 3.3.2)'. Each section has a yellow input field and a 'Show Guidance' link. At the bottom, it indicates '11 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

III. **Task** Complete CMMC Awareness and Training Worksheet

Complete the **CMMC Awareness and Training Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details in the 'Compliance Manager > To Do > Details' view. It features a 'Task' header with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Awareness and Training Worksheet'. The description states: 'Complete the worksheet to assess compliance with the Awareness and Training control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' An orange button labeled 'Go to Form: CMMC - Awareness and Training Worksheet' is present. At the bottom is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- The status of security awareness training at the organization
- The status of role-based security awareness training at the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, and Settings. The main content area is titled 'CMMC Awareness and Training Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for the CMMC – Awareness and Training (AT) control domain. It lists two tasks: 1.1 Security Awareness Training (CMMC Ctrl: AT.2.056) and 1.2 Insider Threat Awareness Training (CMMC Ctrl: AT.3.058). Each task has a description, a 'Show Guidance' link, and a large yellow input field. At the bottom, it indicates '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

IV. **Task** Complete CMMC Configuration Management Worksheet

Complete the **CMMC Configuration Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' card with the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information card titled 'Complete CMMC – Configuration Management Worksheet' with an 'i' icon. The card contains the instruction: 'Complete the worksheet to assess compliance with the Configuration Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the information card is an orange button labeled 'Go to Form: CMMC - Configuration Management Worksheet'. Below the information card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Establish configuration baselines: Ensure principle of least functionality is employed; restrictions on user-installed software.
- Configuration change management: Ensure organization analyzes security configuration changes and establishes and enforces baseline security settings.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Configuration Management Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Configuration Management (CM) control domain. This worksheet should be completed by an Internal Auditor.' It lists two sections: '1 CO13 - ESTABLISH CONFIGURATION BASELINES (2 REQUIRED REMAINING)' and '1.1 Baseline Configuration - CMMC Ctrl: CM.2.061 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.1)'. Below this is a question: 'Are baseline configurations developed, documented, and maintained for each information system type?' followed by a yellow input field. A second section '1.2 Least Functionality - System Configuration - CMMC Ctrl: CM.2.062 - Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.6)' is also present with a similar question and input field. At the bottom, it says '9 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

V. **Task** Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – Identification and Authentication Worksheet'. The main text reads: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button that says 'Go to Form: CMMC - Identification and Authentication Worksheet'. Below the card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content is titled 'Complete the following worksheet regarding the compliance with the CMMC - Identification and Authentication (3A) control domain. This worksheet should be completed by an Internal Auditor'. Below this is a section '1 C315- GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)'. It contains three numbered items: 1.1 User Accounts - CMMC Chrt: 1A.1.076 - Identify information system users, processes acting on behalf of users, or devices. (NIST 800-57 Rev. 2 Chrt Ref: 3.5.5); 1.2 Identify Users - CMMC Chrt: 1A.1.077 - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (NIST 800-57 Rev. 2 Chrt Ref: 3.5.2); and 1.3 Password Complexity - CMMC Chrt: 1A.2.078 - Enforce a minimum password complexity and change of characters when new passwords are created. (NIST 800-57 Rev. 2 Chrt Ref: 3.5.7). Each item has a 'Show Guidance' link and a yellow input field. At the bottom, it says '11 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

VI. **Task** Complete CMMC Incident Response Worksheet

Complete the **CMMC Incident Response Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details in the Compliance Manager interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A blue 'Task' label is followed by the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section with an information icon and the title 'Complete CMMC - Incident Response Worksheet'. The text reads: 'Complete the worksheet to assess compliance with the Incident Response control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Incident Response Worksheet'. At the bottom is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Detail the organization's plan for handling a security incident, including planning, responding, reporting, analyzing, and testing.

The screenshot shows the 'CMMC Incident Response Worksheet' within the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area has a breadcrumb trail 'Compliance Manager > Assessments > Inform' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below this is a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', and 'Download'. A status bar indicates '7 required remaining'. The worksheet content includes instructions to complete the worksheet for the 'Incident Response (IR)' control domain, followed by two sections: '1.1 Incident Handling - CMMC Ctrl: IR.2.092' and '2.1 Incident Detection and Reporting - CMMC Ctrl: IR.2.093'. Each section contains a text input field and a 'Show Guidance' link. At the bottom right are 'Save', 'Save and Return', and 'Return' buttons.

VII. **Task** Complete CMMC Maintenance Worksheet

Complete the **CMMC Maintenance Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card titled 'Complete CMMC - Maintenance Worksheet' under the breadcrumb 'Compliance Manager > To Do > Details'. The card includes a 'Task' icon and a message: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the task title. The description states: 'Complete the worksheet to assess compliance with the Maintenance control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button reads 'Go to Form: CMMC - Maintenance Worksheet'. At the bottom left is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Management of IT maintenance tools and management of IT personnel
- Multifactor authentication for remote access maintenance tools

The screenshot shows the 'CMMC Maintenance Worksheet' form within the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area has a breadcrumb trail 'Compliance Manager > Assessments > InfoForm' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below the header, there are buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The form content includes a note: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Maintenance (PA) control domain. This worksheet should be completed by an Internal Auditor.' It also states '1 C021 - MANAGE MAINTENANCE IS REQUIRED REMAINING'. Three sections are visible: 1.1 Maintenance Tasks - CMMC Ctrl: MA.2.111 - Perform maintenance on organizational systems, 1.2 Controlled Maintenance - CMMC Ctrl: MA.2.112 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance, and 1.3 Nonlocal Maintenance - CMMC Ctrl: MA.2.113 - Require multifactor authentication to establish nonlocal maintenance sessions. Each section has a 'Show Guidance' link and a yellow input field. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

VIII. **Task** Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' icon and the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Media Protection Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is an orange button labeled 'Go to Form: CMMC - Media Protection Worksheet'. At the bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Media Protection Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a message states: 'Complete the following worksheet regarding the compliance with the CMMC – Media Protection (MP) control domain. This worksheet should be completed by an Internal Auditor.' A red banner indicates '1 CO23 - PROTECT AND CONTROL MEDIA IS REQUIRED REMAINING'. Three sections are visible: 1.1 Protect and Control - CMMC Ctrl: MP.2.120 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital, (NIST 800-57 Rev. 2 Ctl Ref: 3.8.1), 1.2 Protect and Control - CMMC Ctrl: MP.2.120 - Limit access to CUI on system media to authorized users, (NIST 800-57 Rev. 2 Ctl Ref: 3.8.2), and 1.3 Protect and Control - CMMC Ctrl: MP.2.121 - Control the use of removable media on system components, (NIST 800-57 Rev. 2 Ctl Ref: 3.8.7). Each section has a 'Show Guidance' link and a yellow input field. At the bottom, it says '8 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

IX. **Task** Complete CMMC Personnel Security Worksheet

Complete the **CMMC Personnel Security Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' card with the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information card titled 'Complete CMMC – Personnel Security Worksheet' with an icon. The text inside says: 'Complete the worksheet to assess compliance with the Personnel Security control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' An orange button labeled 'Go to Form: CMMC - Personnel Security Worksheet' is present. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Procedures to screen individuals before employment and access to sensitive data
- Procedures to restrict employee data access after they leave the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Personnel Security Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', '14 Items Other', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Personnel Security (PS) control domain. This worksheet should be completed by an Internal Auditor.' It lists two sections: '1 CO26 - SCREEN PERSONNEL (1 REQUIRED REMAINING)' and '2 CO27 - PROTECT CUI DURING PERSONNEL ACTIONS (1 REQUIRED REMAINING)'. Each section contains a specific control (e.g., '1.1 Personnel Screening - CMMC Ctrl PS.2.127') and a question. Below each question is a yellow input field. At the bottom, it says '2 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

X. **Task** Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'To Do' task card in the 'Compliance Manager' interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. The card has a 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Physical Protection Worksheet' with an information icon. The description reads: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of this section is an orange button that says 'Go to Form: CMMC - Physical Protection Worksheet'. At the very bottom of the card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Physical Protection Worksheet' under the 'Assessments' > 'Inform' path. It includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 CO28 - LIMIT PHYSICAL ACCESS (6 REQUIRED REMAINING)' and instructions: 'Complete the following worksheet regarding the compliance with the CMMC - Physical Protection (PE) control domain. This worksheet should be completed by an Internal Auditor'. It lists three tasks: 1.1 Control Physical Access, 1.2 Visitor Access Monitoring, and 1.3 Access Audit Logs, each with a description and a 'Show Guidance' link. At the bottom, it indicates '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XI. **Task** Complete CMMC Recovery Worksheet

Complete the CMMC Recovery worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Recovery Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Recovery control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is an orange button labeled 'Go to Form: CMMC - Recovery Worksheet' and a grey button with a checkmark labeled 'Mark Complete' at the bottom.

Specifically, this worksheet asks you to examine:

- Regular performance and testing of data backups
- Protection of CUI data after backup

The screenshot shows the 'CMMC Recovery Worksheet' in the Compliance Manager application. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and a list of tasks. The first task is '1.1 Regularly Perform and Test Data Backups - CMMC Ctl: RE.3.137 - Regularly perform and test data backups.' It includes a description, a 'Show Guidance' link, and a progress bar. The second task is '1.2 Protect CUI Backups - CMMC Ctl: RE.3.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctl Ref: 3.8.9)' It also includes a description, a 'Show Guidance' link, and a progress bar. The third task is '1.3 Perform Comprehensive Backups - CMMC Ctl: RE.3.139 - Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.' It includes a description and a progress bar. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return'.

XII. **Task** Complete CMMC Risk Management Worksheet

Complete the **CMMC Risk Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'To Do' list in the Compliance Manager application. The breadcrumb navigation is 'Compliance Manager > To Do > Details'. The first item is a task: 'This is a task that requires an action to be taken. See below for details.' Below this is a task card titled 'Complete CMMC - Risk Management Worksheet' with an information icon. The card contains the text: 'Complete the worksheet to assess compliance with the Risk Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Risk Management Worksheet'. At the bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Risk and vulnerability assessment
- Vulnerability scanning
- Vulnerability remediation

The screenshot shows the 'CMMC Risk Management Worksheet' in the Compliance Manager application. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Risk Management Worksheet' and includes a search bar and a 'Select Assessment' dropdown set to 'Current Assessment'. Below the title, there are buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet to document compliance with CMMC controls. It features two sections: '1.1 Risk Assessment - CMMC Ctrl: RM.2.541 - Periodically assess the risk to organizational operations...' and '1.2 Vulnerability Scanning - CMMC Ctrl: RM.2.542 - Scan for vulnerabilities...'. Each section has a yellow input field for responses. At the bottom, it indicates '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XIII. **Task** Complete CMMC Security Assessment Worksheet

Complete the CMMC Security Assessment worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. The left sidebar has navigation links: Home, Compliance Manager, To Do (highlighted), Assessments, Settings, and Audit Log. The main content area shows a breadcrumb trail 'Compliance Manager > To Do > Details'. A blue 'Task' button is followed by the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Security Assessment Worksheet' with an information icon. The text inside this section says: 'Complete the worksheet to assess compliance with the Security Assessment control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button that says 'Go to Form: CMMC - Security Assessment Worksheet'. At the bottom of the section is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Existence of a system security plan
- Assessment of the security plan
- Plans of action against vulnerabilities

The screenshot shows the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The 'Forms' link is selected. The main content area displays the 'CMMC Security Assessment Worksheet'. At the top, there's a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a task description states: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Security Assessment (CA) control domain. This worksheet should be completed by an Internal Auditor.' The worksheet is divided into sections: '1 C034 - DEVELOP AND MANAGE A SYSTEM SECURITY PLAN (1 REQUIRED REMAINING)' and '2 C035 - DEFINE AND MANAGE CONTROLS (3 REQUIRED REMAINING)'. Each section contains a detailed task description and a 'Show Guidance' link. At the bottom, a status bar indicates '5 required remaining' and includes 'Save', 'Save and Return', and 'Return' buttons.

XIV. **Task** Complete CMMC Situational Awareness Worksheet

Complete the **CMMC Situational Awareness Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' workspace. The left sidebar is the same as the previous screenshot. The 'To Do' link is selected. The main content area displays a task card titled 'Complete CMMC - Situational Awareness Worksheet'. The card includes a 'Task' icon and a description: 'Complete the worksheet to assess compliance with the Situational Awareness control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Situational Awareness Worksheet'. At the bottom of the card is a 'Mark Complete' button with a checkmark icon. The top of the workspace shows navigation links: Sites, To Do, Global Settings, and a user profile 'joe-admin-user@rapidfiretools.com'.

Specifically, this worksheet asks you to examine how the organization becomes aware of and/or identifies potential cyber threats.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Situational Awareness Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Info/Details', 'Save', 'Save and Return', and 'Return'. Below these is a section for '1 CO37 - IMPLEMENT THREAT MONITORING (2 REQUIRED REMAINING)'. The first item is '1.1 Threat Monitoring - CMMC Cat: SA.3.3.69 - Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. Has the organization implemented policies and practices to periodically receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders?'. A yellow progress bar is shown below the text. At the bottom, it says '1 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XV. **Task** Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – System and Communications Protection Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button that says 'Go to Form: CMMC - Systems and Communication Protection Worksheet'. Below the card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The 'Forms' option is selected. The main content area displays the 'CMMC System and Communications Protection Worksheet'. At the top, it says 'Compliance Manager > Assessments > Inform'. Below this, there's a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. A note states: 'Complete the following worksheet regarding the compliance with the controls contain within the CMMC - System and Communications Protection (SC) control domain. This worksheet should be completed by an Internal Auditor.' Below the note, there are two sections for questions: '1. CO38 - DEFINE SECURITY REQUIREMENTS FOR SYSTEMS AND COMMUNICATIONS (15 REQUIRED REMAINING)' and '1.1 Collaborative Computing Devices - CMMC Ctrl: SC.2.378 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (NIST 800-571 Rev. 2 Ctrl Ref: 3.33.52)'. Each section has a yellow input field and a 'Show Guidance' link. At the bottom, it says '19 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

XVI. **Task** Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

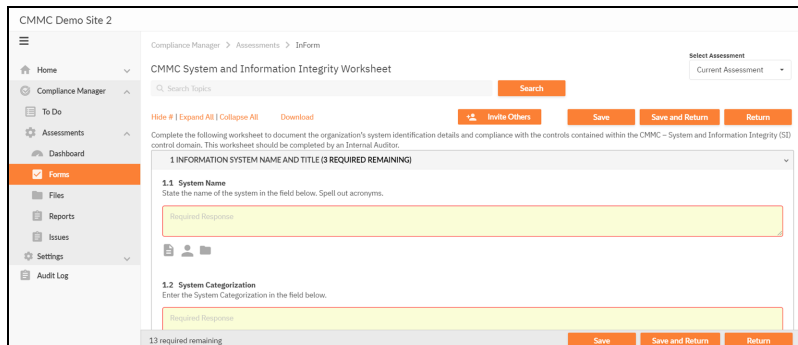
The screenshot shows the 'Task' section in the Compliance Manager interface. At the top, it says 'Compliance Manager > To Do > Details'. Below this, there's a 'Task' box with the text: 'This is a task that requires an action to be taken. See below for details.' Below the task box, there's an information icon and the title 'Complete CMMC - System and Information Integrity Worksheet'. The text below the title says: 'Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text, there's an orange button that says 'Go to Form: CMMC - System and Information Integrity Worksheet'. At the bottom, there's a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans for Federal Information Systems," page 19, section 3, "Plan

Development." This document is currently available at:
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

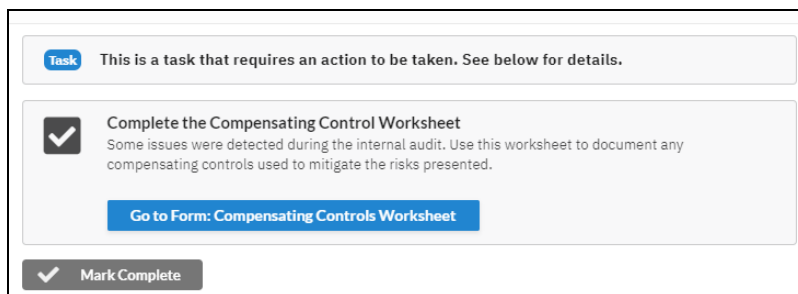


Step 9 — Document Compensating Controls

Task Complete the Compensating Controls Worksheet.

Use this worksheet to document any compensating controls used to mitigate the risks detected during the assessment.

1. Click the **Go To Form** button to open the worksheet.



2. Enter your responses for the worksheet. Here you can document any false positives. You can also indicate if you have taken measures to reduce or avoid any issues identified in the assessment that might not otherwise appear in your assessment documentation.

The screenshot shows the 'Compensating Control Worksheet' interface in the Compliance Manager application. The breadcrumb trail at the top reads 'Compliance Manager > Assessments > In-Form'. A 'Current Assessment' dropdown menu is located in the top right corner. The main title 'Compensating Control Worksheet' is followed by a search bar and a 'Search' button. Below this are links for 'Hide #', 'Expand All', 'Collapse All', and a 'Download' button. On the right side, there are 'Save' and 'Save and Return' buttons. The content area displays two verified incorrect responses. The first, '1.1 Verified Incorrect response: Sensitive Data (PII) found', includes a description, a 'Valid' button, and a 'Mitigated through Compensating Control' section with a 'Review Individual Entries' link. The second, '2.1 Verified Incorrect response: Personal Data (PII) found', also includes a description, a 'Valid' button, and a 'False Positive' section. At the bottom left, there are icons for a document, a person, and a folder.

3. When are finished, return to the To Do item and click **Mark Complete**.

Step 10 — Generate CMMC Assessment Reports

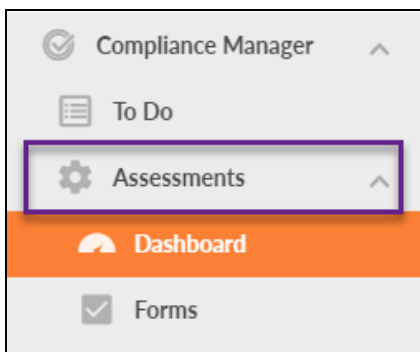
Task Review Final Reports.

After documenting the compensating controls, the assessment reports and supporting documentation will become available for review.

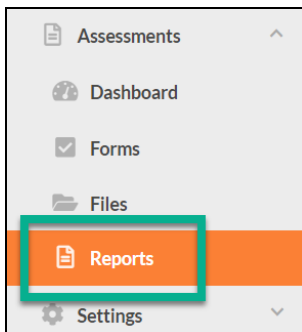
Note: It may take several minutes for the reports to appear once you reach this step.

To review the reports and findings:

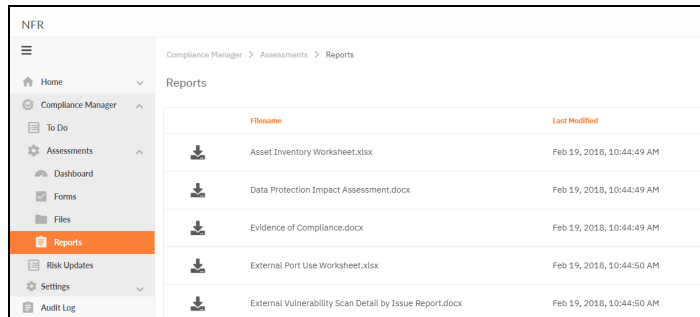
1. From your Site, go to **Compliance Manager > Assessments**.



2. Click **Reports** from the left menu to access a list of generated reports.



3. The Reports page will appear. Click the download icon next to the report that you wish to download and view.

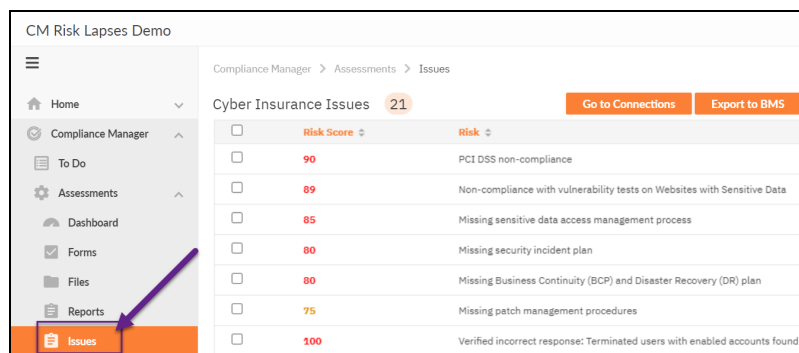


Filename	Last Modified
Asset Inventory Worksheet.xlsx	Feb 19, 2018, 10:44:49 AM
Data Protection Impact Assessment.docx	Feb 19, 2018, 10:44:49 AM
Evidence of Compliance.docx	Feb 19, 2018, 10:44:49 AM
External Port Use Worksheet.xlsx	Feb 19, 2018, 10:44:50 AM
External Vulnerability Scan Detail by Issue Report.docx	Feb 19, 2018, 10:44:50 AM

- Once you have reviewed the reports, click **Mark Complete** on the task details page.

Optional Task: Export Issues to Kaseya BMS

Once you generate assessment reports and review them, you can view specific issues identified in the assessment — organized by risk score — from the **Issues** tab. These issues supplement the detailed data in your reports with immediate action items — and likewise allow you to export these issues as tickets to Kaseya BMS.



Risk Score	Risk
90	PCI DSS non-compliance
89	Non-compliance with vulnerability tests on Websites with Sensitive Data
85	Missing sensitive data access management process
80	Missing security incident plan
80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan
75	Missing patch management procedures
100	Verified incorrect response: Terminated users with enabled accounts found

To do this:


Step 1 — Gather Credentials and Set Up Kaseya BMS

Before you begin, you will need:

- Valid Login Credentials for RapidFire Tools Portal
- A RapidFire Tools Portal Compliance Manager "Site" for which you wish to export

tickets

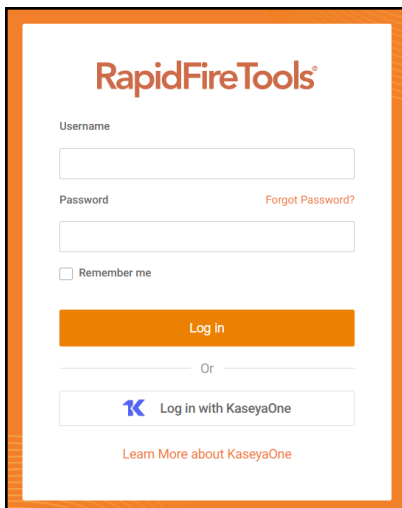
- Valid Login Credentials and details for Kaseya BMS (refer to the table below)

PSA System	PSA Prerequisites
	<ul style="list-style-type: none">• Kaseya Username• Kaseya Password• Kaseya Tenant (i.e. company name)• Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

Step 2 — Set Up a Connection to your Kaseya BMS

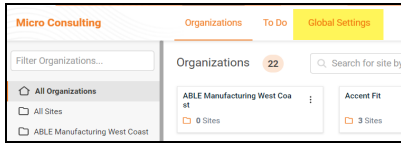
Follow these steps to set up a Connection to Kaseya BMS.

1. Visit <https://www.youritportal.com> and log into the RapidFire Tools Portal.

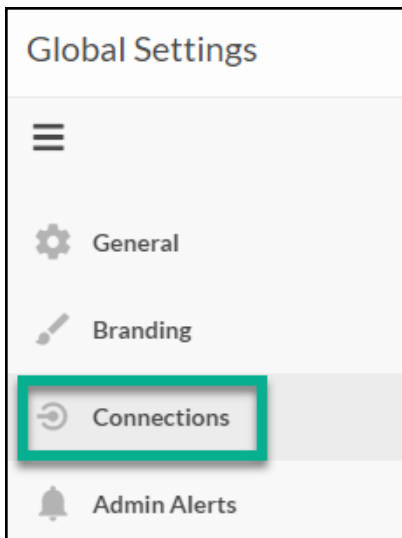
The image shows the login page for RapidFireTools. At the top is the "RapidFireTools" logo. Below it are two input fields: "Username" and "Password". To the right of the "Password" field is a link that says "Forgot Password?". Below the "Password" field is a checkbox labeled "Remember me". A large orange "Log in" button is positioned below the "Remember me" checkbox. Below the "Log in" button is a horizontal line with the word "Or" in the center. Below the line is a button with the Kaseya logo and the text "Log in with KaseyaOne". At the bottom of the page is a link that says "Learn More about KaseyaOne".

Note: In order to configure the Settings in the Portal, you must have the **All** or **Admin** global access level.

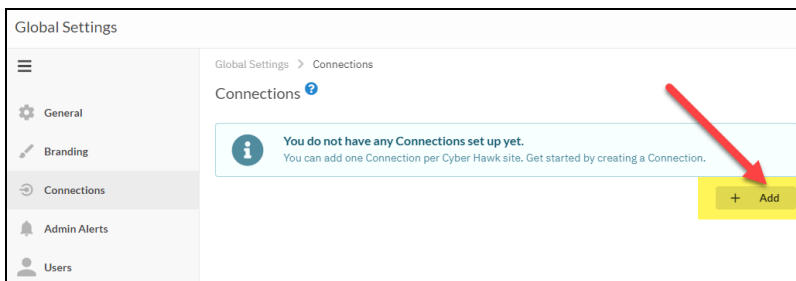
2. Click **Global Settings**.



3. Click **Connections**.



4. Click **Add** to create a new Ticketing System/PSA Connection.



5. In the Setup New Connection window, select **Connection Type** and choose **Kaseya BMS**.

Note: Compliance Manager can only be integrated with Kaseya BMS at this time.

Add Connection

Add New Connection

Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.

Connection Type *

– Choose Connection Type –

- Autotask
- ConnectWise
- ConnectWise REST
- Kaseya BMS
- TigerPaw
- Dark Web ID


Cancel Test Login


6. Then enter the information required to set up the Connection.

This information will include:

- Username and Password
- API URL
- Tenant name (Company name)

Add Connection

**Setup New Connection**
Integrating with PSA and ticketing systems allows automated creation of tickets on a per-site basis. Enter the appropriate ticketing API credentials below.

 Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.

Connection Type *

Username *

Password *


.....

Tenant *

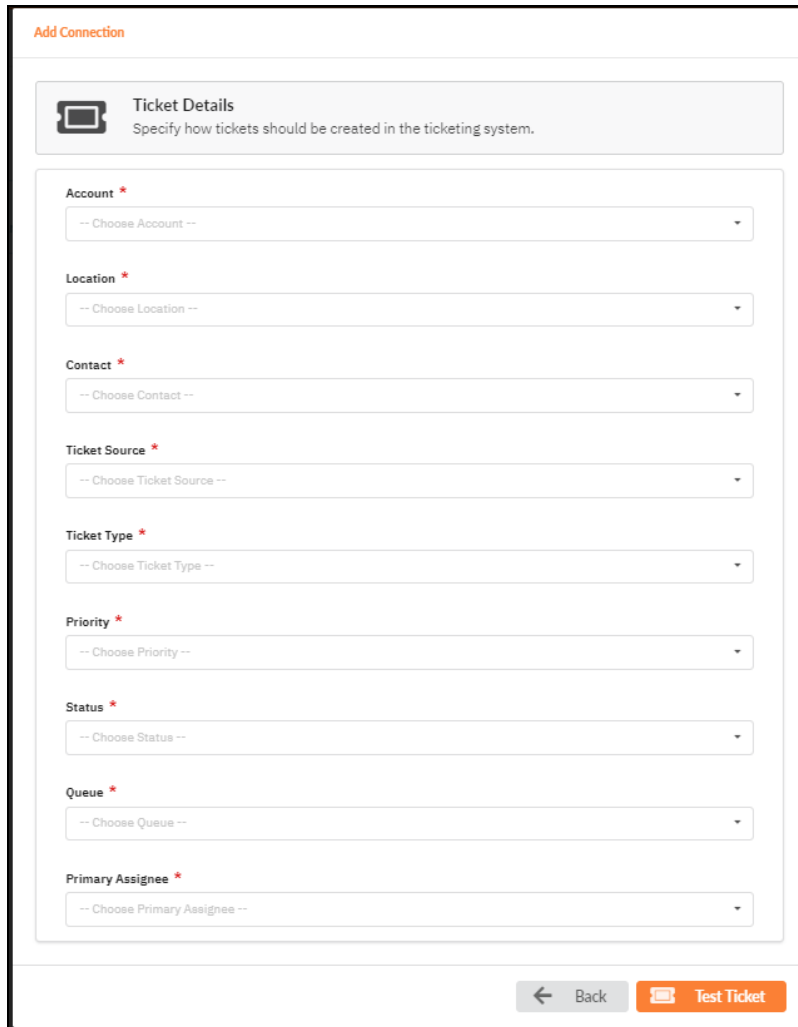
NFR RapidFire Tools

API URL *

Cancel



7. Click **Test Login** button to test your Connection login. After a successful test login, the second Add Connection Ticket Details window will be displayed.
8. Continue creating your Connection by entering in the necessary Ticket Details.





The screenshot shows a web interface titled "Add Connection" in orange text. Below the title is a section labeled "Ticket Details" with a sub-header "Specify how tickets should be created in the ticketing system." This section contains nine dropdown menus, each with a red asterisk indicating it is required. The fields are: Account, Location, Contact, Ticket Source, Ticket Type, Priority, Status, Queue, and Primary Assignee. Each dropdown menu has a placeholder text "-- Choose [Field Name] --". At the bottom right of the form, there are two buttons: a grey "Back" button with a left arrow and an orange "Test Ticket" button with a ticket icon.

Click **Test Ticket**. The Add Connection Settings Confirmation window will be displayed after the Test Ticket process is successful.

9. In the Add Connection Confirm Settings window presented, enter a **Connection Name**.
10. Review the Connection's configuration details and click **Save**.


Add Connection

 **Confirm Details**
Please confirm the information below before saving your new Connection.



 **Connection**

Connection Name *


Type	Kaseya BMS
Login	<input type="password"/>

 **Ticketing**

Account	NFR RapidFire Tools	Location	NFR RapidFire Tools
Contact	Leo Tolstoy	Ticket Source	Verbal
Ticket Type	Problem	Priority	Medium
Status	Completed	Queue	Level Three Support
Primary Assignee	RFT Test		

 Back  Save

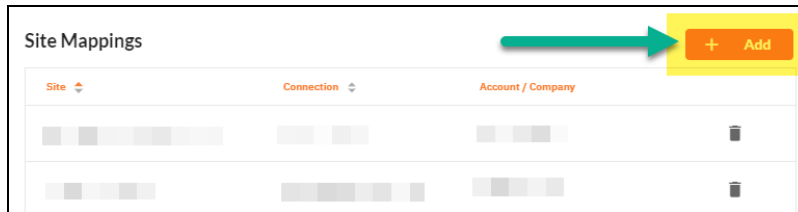
The new Connection created will be listed in the Portal's Connection list.

Connections ⓘ			
Your Connections			 Add
Name ↕	Type ↕	Login ↕	
BMS Export CM Issues	Kaseya BMS	<input type="password"/>	 

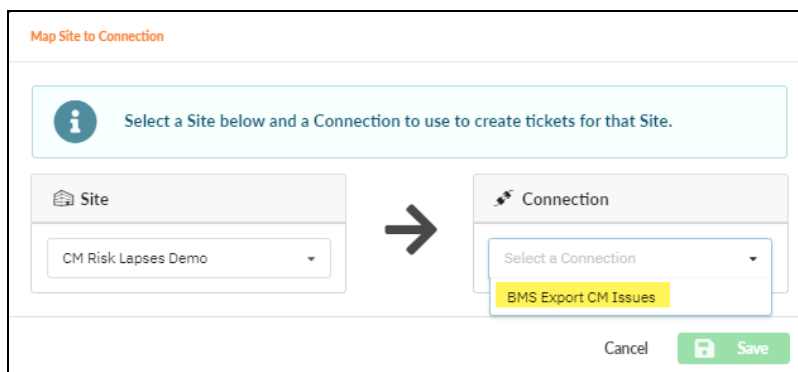
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS

Follow these steps to map a Kaseya BMS Connection to the RapidFire Tools Portal Site associated with your Compliance Manager assessment.

1. From the **Global Settings > Connections** menu, scroll down and click **Add** under Site Mappings. The Map Site to Connection window will be displayed.

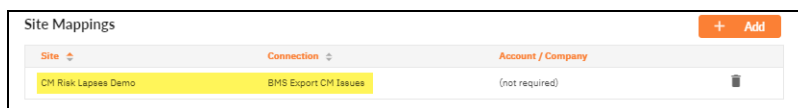


2. Select the RapidFire Tools Portal Compliance Manager **Site** you want to assign to the Kaseya BMS Integration.
3. Next, **select the name of the Connection** that you want use to link the Site to Kaseya BMS.



4. Click **Save**. The Site's mapping will be saved and listed in the Site Mappings list.

You can now export Issues as tickets for the RapidFire Tools Portal Site you selected.

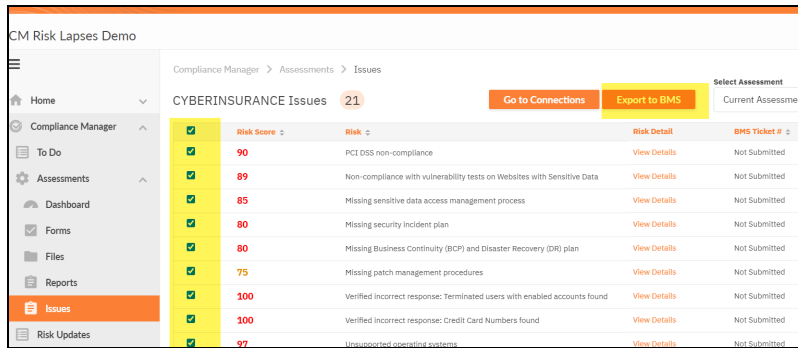


Step 4 — Export Issues to Kaseya BMS

The final step is to select issues and export them. To do this:

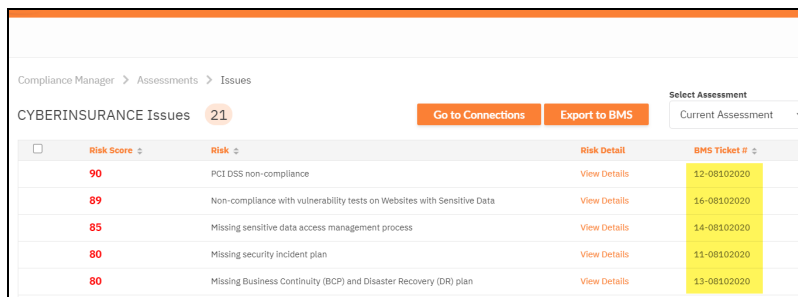
1. Navigate to the site with the issues you want to export. Go to **Compliance Manager > Assessment > Issues**.
2. Check the box next to each issue to be exported.

3. Click **Export to BMS** and confirm.



	Risk Score	Risk	Risk Detail	BMS Ticket #
✓	90	PCI DSS non-compliance	View Details	Not Submitted
✓	89	Non-compliance with vulnerability tests on Websites with Sensitive Data	View Details	Not Submitted
✓	85	Missing sensitive data access management process	View Details	Not Submitted
✓	80	Missing security incident plan	View Details	Not Submitted
✓	80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan	View Details	Not Submitted
✓	75	Missing patch management procedures	View Details	Not Submitted
✓	100	Verified incorrect response: Terminated users with enabled accounts found	View Details	Not Submitted
✓	100	Verified incorrect response: Credit Card Numbers found	View Details	Not Submitted
✓	97	Unsupported operating systems	View Details	Not Submitted

Each successfully exported issue will receive a ticket number. The issues will now be available as tickets in Kaseya BMS.



	Risk Score	Risk	Risk Detail	BMS Ticket #
	90	PCI DSS non-compliance	View Details	12-08102020
	89	Non-compliance with vulnerability tests on Websites with Sensitive Data	View Details	16-08102020
	85	Missing sensitive data access management process	View Details	14-08102020
	80	Missing security incident plan	View Details	11-08102020
	80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan	View Details	13-08102020

Note: Once the ticket is exported, you can continue to view its details, but you cannot export it twice.

Step 11 — Complete and Archive your CMMC Assessment

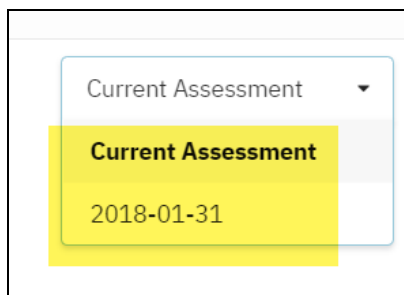
Task CMMC Assessment Complete.

In this step, after you have reviewed your CMMC assessment reports, the CMMC assessment will be complete. Compliance Manager will also note the number of compliance and security issues detailed for further review in the Risk Assessment report.

Archiving Assessments

When you complete an assessment, that assessment will be archived. You can review the assessment and the generated reports and compliance documentation. To do this:

1. Navigate to the **Compliance Manager > Assessments** tab.
2. Click on the drop-down menu from the right side of the screen.



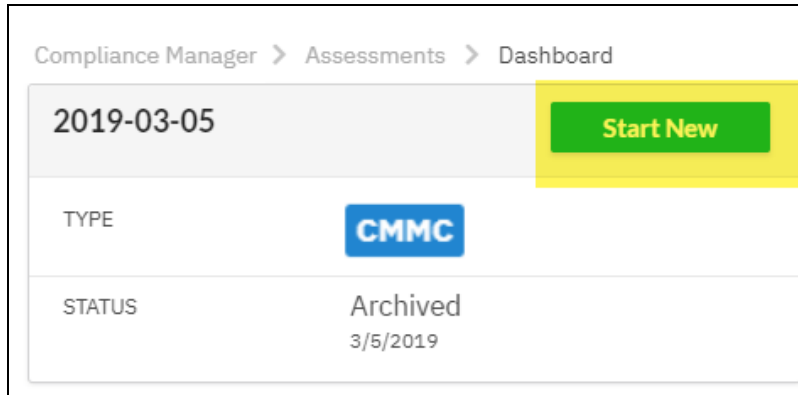
3. Select the archived assessment you wish to review.

Note: Your archived assessment will be named: **YYYY-MM-DD** where the date is the start date of the assessment.

Step 12 — Start a New CMMC after Completing a Previous Assessment

To start a new assessment, follow these steps:

1. Go to **Compliance Manager > Assessments > Dashboard**.
2. Click **Start New**.



Your To Do List will be reset. The **Start CMMC Assessment** To Do item will be added to your To Do list.

CMMC Assessment Reports

Compliance Manager for CMMC can generate the following reports and supporting documents:

CMMC Compliance Reports

These reports show where you are in achieving CMMC compliance. In addition, these documents identify and prioritize issues that must be remediated to address CMMC related security vulnerabilities through ongoing managed services.

Report Type	Description	Level 1	Level 2	Level 3
CMMC Assessor Checklist	The CMMC Assessor Checklist gives you a high-level overview of how well the organization complies with the CMMC (Cybersecurity Maturity Model Certification) requirements. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.	✓	✓	✓
CMMC Evidence of Compliance	Compiles compliance information from automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the CMMC Assessor Checklist with real data.	✓	✓	✓
CMMC Risk Analysis	CMMC Risk Analysis is the foundation for the entire CMMC compliance and IT security program. The CMMC Risk Analysis identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of sensitive data at rest and/or during its transmission.	✓	✓	✓
CMMC Risk Treatment Plan	Based on the findings in the CMMC	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
	Compliance Assessment, the organization must create a Risk Treatment Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, CMMC Manager provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Treatment plan defines the strategies and tactics the organization will use to address its risks.			
CUI Plan of Actions and Milestones Report*	The CUI Plan of Action is organized by the NIST security control requirements and cross references the CMMC control domains. It details the status of implementation for each control, and provides suggestions for resolving the issues identified. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓
CUI System Security Plan*	This document supplements the Risk Analysis, Risk Treatment Plan, and NIST SP 800 - 171 DoD Assessment Scoring report and offers substantiation and verification of compliance with control requirements. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓
NIST 800 171 Scoring Supplement Worksheet*	The optional NIST 800-171 Scoring Supplement allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in		✓	

Report Type	Description	Level 1	Level 2	Level 3
	the form of a DoD Assessment Score. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>			
NIST SP 800 171 DoD Assessment Score Report*	This report details the DoD Assessment Score as per the DoD Assessment methodology. It details the control point value deductions, as well as the implementation status for each required control. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓

Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
CMMC Full Detail Excel Export	The CMMC Full Detail Excel Export includes every detail uncovered during the CMMC assessment's network and computer endpoint scanning process. Details are presented in line-item fashion in an editable Excel workbook document. The report is organized by titled worksheets to help you locate the specific findings of interest, and problem areas are conveniently highlighted in red, making it easy to spot individual problems to be rectified
CMMC Login History Report	This report presents user login history by computer to enable workforce members responsible for IT Security to audit access to computers connected to a company's network. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive “CUI” computers that are used to collect, process, transmit, or store CUI for failed login attempts.
CMMC Windows Patch Assurance Report	The CMMC Windows Patch Assurance Report helps verify the effectiveness of the client's patch management program. The report uses scan data to detail which patches are missing on the network.
External Vulnerability Scan Detail by Issue	Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

Worksheets by Assessment Level

Report Type	Description	Level 1	Level 2	Level 3
CMMC Access Control Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Access Control” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Antivirus Verification Worksheet	Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. The Anti-virus Verification Worksheet details whether each endpoint on the network has anti-virus software installed. It also displays the type of anti-virus software.	✓	✓	✓
CMMC Application Inventory Worksheet	This worksheet is used to document the “necessity” of the applications identified as being installed on the computer endpoints operating within the network.	✓	✓	✓
CMMC Asset Inventory Worksheet	The Asset Inventory Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the asset owner, acceptable use, environment, backup agent status, as well as device and asset criticality classification. The asset criticality classification is used to determine the risk to the organization in the event of a security incident where the asset’s access or availability is compromised.	✓	✓	✓
CMMC Asset Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Asset Management Worksheet” control domain requirements that cannot be discovered and assessed through			✓

Report Type	Description	Level 1	Level 2	Level 3
	automated scans.			
CMMC Audit and Accountability Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Audit and Accountability” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Awareness and Training Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Awareness and Training” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Configuration Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Configuration Management” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC External Information System Worksheet	This worksheet is used to document external information systems used by your organization. Add entries for each external information system along with a description, purpose for using the system, name of the business owner of the system, along with its criticality. Examples of external information systems include Salesforce, QuickBooks Online, and Office 365.	✓	✓	✓
CMMC External Port Use Worksheet	This worksheet allows you to document business justifications for all of the allowed external ports, the protocol configured to use a specific port, and the	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
	documentation of any insecure configurations implemented and in use for a given protocol.			
CMMC Identification and Authentication Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Identification and Authentication” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Incident Response Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Incident Response” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Maintenance Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Maintenance” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Media Protection Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Media Protection” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Personnel Security Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Personnel Security” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓

Report Type	Description	Level 1	Level 2	Level 3
CMMC Physical Protection Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Physical Protection” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Recovery Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “recovery” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Risk Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Risk Management” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Security Assessment Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Security Assessment” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Situation Awareness Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Situation Awareness Worksheet” control domain requirements that cannot be discovered and assessed through automated scans.			✓
CMMC System and Communications Protection	This worksheet is used to collect information required to demonstrate compliance with the CMMC “System	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
Worksheet	and Communications Protection” control domain requirements that cannot be discovered and assessed through automated scans.			
CMMC System and Information Integrity Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “System and Information Integrity” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC User Access Review Worksheet	The User Access Worksheet is used to augment the user data that was collected during the internal network scan. Complete the worksheet to provide the additional information requested.	✓	✓	✓
NIST 800 171 Scoring Supplement Worksheet	The optional NIST 800-171 Scoring Supplement allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in the form of a DoD Assessment Score.		✓	

CMMC Risk Update Assessment Reports

Report Type	Description
CMMC Change Summary Report	Every time you use Compliance Manager for CMMC to run a CMMC Risk Update Assessment on a given network, Compliance Manager for CMMC generates the CMMC Change Summary report. This report compares the results the last Full CMMC Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process. This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.
CMMC Risk Treatment Plan Update	Based on the findings in the CMMC Risk Update Assessment, the organization must create a CMMC Risk Treatment Plan with tasks required to minimize, avoid, or respond to identified risks to IT security. The CMMC Risk Treatment Plan Update contains a list of tasks that can be executed to mitigate identified IT Security risks.
CMMC Risk Analysis Update	The CMMC Risk Analysis Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of IT network security. The CMMC Risk Analysis Update identifies what protections are in place and where there is a need for more. The CMMC Risk Analysis Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of sensitive or confidential information at rest and/or during its transmission.
External Vulnerability Scan Detail**	Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

Appendices

Refer to the appendices listed below for the supplementary information referenced in this user guide:

<u>Pre-Scan Network Configuration Checklist</u>	134
Checklist for Domain Environments	134
Checklist for Workgroup Environments	136
<u>CMMC To Do Task Complete List</u>	139

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation – and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

Note: You must have the .NET 4.6.2 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
GPO Configuration for Windows Firewall (Inbound Rules)	
<input type="checkbox"/>	<p>Allow <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none">• Windows Management Instrumentation (ASync-In)• Windows Management Instrumentation (WMI-In)• Windows Management Instrumentation (DCOM-In)
<input type="checkbox"/>	<p>Allow <i>File and printer sharing</i> to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none">• File and Printer Sharing (NB-Name-In)• File and Printer Sharing (SMB-In)• File and Printer Sharing (NB-Session-In)
<input type="checkbox"/>	<p>Enable <i>Remote Registry</i> “read only” access on computers targeted for scanning.</p>

Complete	Domain Configuration
	<div data-bbox="427 296 1382 407"> <p>Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.</p> </div>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p> <ul style="list-style-type: none"> • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request <div data-bbox="427 863 1382 974"> <p>Note: ICMP requests are used to detect active Windows computers and network devices to scan.</p> </div>
GPO Configuration for Windows Services	
<input type="checkbox"/>	<p><i>Windows Management Instrumentation (WMI)</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Windows Update Service</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Registry</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Procedure Call</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
Network Shares	
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Admin\$</i> must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

Complete	Domain Configuration
3rd Party Firewalls	
<input type="checkbox"/>	<ul style="list-style-type: none"> • Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. <div style="border: 1px solid #0070c0; padding: 5px; margin-top: 10px;"> Note: This is a requirement for both Active Directory and Workgroup Networks. </div>

Checklist for Workgroup Environments

Before you perform a workgroup assessment, run the following PowerShell commands on the target network and the machine that will perform the scan. These three configurations should help you avoid most issues in a workgroup environment. Each command is followed by an explanation and link to Microsoft documentation.

1. `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`

By default, UAC only allows remote administration tasks to be performed by the Built-in Administrator account. To work around this, this command sets the LocalAccountTokenFilterPolicy registry key to 1. This allows any local admin to perform remote administrative tasks (i.e. access to system shares C\$, Admin\$, etc.).

<https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows>

2. `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes`

This command creates an Inbound firewall rule to allow access to the WMI service and namespaces.

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista>

3. `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`

This command creates an Inbound firewall rule which enables File and Printer Sharing on the machine. File and printer sharing is required in order to access the Admin\$ share on remote machines.

<https://answers.microsoft.com/en-us/windows/forum/all/turning-on-file-and-printer-sharing-windows-10/bb3066eb-f589-4021-8f71-617e70854354>

You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

Complete?	Workgroup Configuration
	Network Settings
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Admin\$</i> must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>File and printer sharing</i> must be enabled on the computers you wish to scan
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</i> <ul style="list-style-type: none"> • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
<input type="checkbox"/>	<ul style="list-style-type: none"> • Workgroup computer administrator user account credentials. <div> Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard. </div>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p>

Complete?	Workgroup Configuration
	<ul style="list-style-type: none">• operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices• to send ICMP echo reply messages in response to an ICMP echo request <div data-bbox="443 491 1325 600">Note: ICMP requests are used to detect active Windows computers and network devices to scan.</div>

CMMC To Do Task Complete List

The list below outlines all To Do tasks in the CMMC Assessment To Do list.

Note: The items below may appear in a different order in your To Do list. This depends on the order in which you choose to complete certain tasks.

	Task	Project Role
<input type="checkbox"/>	Create additional users and assign to roles (Home tab > Settings > Users; Roles) <i>Add and invite users to participate in the assessment. Then assign these users to project roles.</i>	Site Admin
<input type="checkbox"/>	Set up Report Preferences (Compliance Manager tab > Settings > Report Preferences) <i>Configure the reports for the Site that will be generated at the end of the assessment. This includes visual elements and client details.</i>	Site Admin
<input type="checkbox"/>	Install Compliance Manager Server (Installed on client network) <i>Compliance Manager Server on the target network.</i>	Technician
<input type="checkbox"/>	Configure Server Scan Settings (Compliance Manager tab > Settings > Scan Settings) <i>Once server is installed, enter information to set up scans.</i>	Technician
<input type="checkbox"/>	Start CMMC Assessment (Compliance Manager tab > To Do) <i>Initial start of assessment. Starts automated scans and generates forms to complete.</i>	Internal Auditor
<input type="checkbox"/>	Running Pre-Scan Analysis (Automated Scan) <i>The server will check for issues that might prevent a complete network scan.</i>	Compliance Manager Server
<input type="checkbox"/>	Review Pre-Scan Analysis Results and Recommendations (Compliance Manager tab > To Do)	Technician

	Task	Project Role
	<i>Review and fix potential scan problems before starting the internal scans.</i>	
<input type="checkbox"/>	Running the Automated Internal Network Scan (Automated Scan) <i>An automated scan will begin on the client's internal network.</i>	Compliance Manager Server
<input type="checkbox"/>	Running Local Scan of Remote Computers (Automated Scan) <i>An automated scan will begin on the client's internal network targeting remote computers.</i>	Compliance Manager Server
<input type="checkbox"/>	Unable to scan all selected systems (Compliance Manager tab > To Do) <i>Perform and upload computer scans on machines that could not be reached during the internal scan.</i>	Technician
<input type="checkbox"/>	Run Local Data Collector (optional) (Compliance Manager tab > To Do) <i>Perform and upload computer scans on machines that could not be reached during the internal scan.</i>	Technician
<input type="checkbox"/>	Running the Automated External Vulnerability Scan (Automated Scan) <i>An automated external vulnerability scan will begin on the designated IP addresses.</i>	Compliance Manager Server
<input type="checkbox"/>	Complete External Port Use Worksheet (Compliance Manager tab > To Do) <i>Enter information about external ports discovered during the external scan.</i>	Technician
<input type="checkbox"/>	Complete Antivirus Verification Worksheet (Compliance Manager tab > To Do) <i>Assess</i>	Internal Auditor
<input type="checkbox"/>	Complete User Access Review Worksheet (Compliance Manager tab > To Do) <i>Assess</i>	Internal Auditor

	Task	Project Role
<input type="checkbox"/>	Complete Asset Inventory Worksheet (Compliance Manager tab > To Do) <i>Document any</i>	Internal Auditor
<input type="checkbox"/>	Complete Application Inventory Worksheet (Compliance Manager tab > To Do) <i>Document how</i>	Internal Auditor
<input type="checkbox"/>	Complete External Information System Worksheet (Compliance Manager tab > To Do) <i>Document any</i>	Internal Auditor
<input type="checkbox"/>	Select Level of CMMC Assessment (Compliance Manager tab > To Do) <i>Optionally can choose to add additional worksheets to your assessment to identify additional issues.</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Access Control Worksheet (Level 1 and Level 2) (Compliance Manager tab > To Do) <i>Conduct</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Audit and Accountability Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Conduct an inventory of all .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Awareness and Training Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Conduct an inventory of all</i>	Technician
<input type="checkbox"/>	Complete CMMC Configuration Management Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Select</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Identification and Authentication Worksheet (Level 1 and Level 2) (Automated Scan)	Internal Auditor

	Task	Project Role
	<i>An automated scan of the client network will begin checking for .</i>	
<input type="checkbox"/>	Complete CMMC Maintenance Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Media Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Personnel Security Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Physical Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Recovery Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Risk Management Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Security Assessment Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC System and Communications Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC System and Information Integrity Worksheet (Level 1 and Level 2) (Automated Scan)	Internal Auditor

	Task	Project Role
	<i>An automated scan of the client network will begin checking for .</i>	
<input type="checkbox"/>	Review Final Reports (Compliance Manager tab > To Do) <i>Examine the final reports and supporting documents to demonstrate compliance or begin remediating issues.</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Assessment (Compliance Manager tab > To Do) <i>Finish and archive your CMMC Assessment. You can review the archived documentation at any time.</i>	Internal Auditor