

COMPLIANCE MANAGER GRC™ by RapidFire Tools



USER GUIDE

5/29/2024 2:50 PM

Compliance Manager GRC

Instructions to Perform a Compliance Assessment



+1-678-323-1300



[rapidfiretools.com](https://www.rapidfiretools.com)



support@rapidfiretools.com

Contents

Introduction to Compliance Manager GRC	15
<u>About Compliance Manager GRC: Governance, Risk & Compliance</u>	15
Compliance Manager GRC Sweats the Details, So You Don't Have To	15
A Customizable Compliance Solution	15
Automated Reporting & Custom Documentation	16
Employee and Vendor IT GRC Tracking	16
<u>Compliance Manager GRC Assessment Overview</u>	17
Compliance Assessment Overview	17
Available "Out-of-Box" Standards	17
Network Prerequisites for Assessment Scans	19
<u>Manage Portal Users and Access</u>	20
Manage Users (Global Level)	20
Users and Global Access Roles	21
Add User at Global Level	23
Edit User at Global Level	26
Enable Log In with KaseyaOne	27
Enable Log in with KaseyaOne at Account Level from Global Settings	27
Log in with your KaseyaOne user	30
User Matching Criteria	31
Require Log In with KaseyaOne	31
Important Note	32
Enable Require Log In with KaseyaOne	32
Frequently Asked Questions	34
Enable Automatic User Creation for RapidFire Tools Portal	35
Step 1 – Enable Log in with KaseyaOne at Account Level from Global Settings	35
Step 2 – Enable Automatic User Creation	37
Step 3 – KaseyaOne User Logs into RapidFire Tools Portal	40
Enable Global Two-Factor Authentication (2FA) for Portal Users	41
Step 1 — Master user enables 2FA for all portal users	41
Step 2 — Portal user logs in and sets up 2FA Access	41

Step 3 — Portal Users enter Authentication Code after initial login	43
Change your Password	44
Recover Forgotten Password	46
Log Out of RapidFire Tools Portal	48
Enable Access Groups	49
<u>Set Up Portal Branding</u>	52
Set Custom Portal Theme	53
Set Custom Portal Subdomain	54
Set Custom Company Name	55
Set Custom Company Logo	56
Set Up a Custom Subdomain to Access the RapidFire Tools Portal	58
<u>Portal Administration</u>	59
Set Time Zone	59
Report Date Format (Global Settings)	60
Admin Alerts (RapidFire Tools Portal)	62
Admin Alerts: Global Settings vs. Site Settings	62
Configure Admin Alerts	62
Delete a Site	63
Import IT Glue Organizations	65
Step 1 — Create and Copy API Key in IT Glue	65
Step 2 — Enable Connection to IT Glue from Portal Global Settings	66
Step 3 — Set Up Organizations	69
Step 4 — Synchronize Org Names with IT Glue	71
Pause Org Name Synchronization	71
Import IT Glue Orgs when Creating New Organizations	72
Create an API Key	74
<u>Set Up Compliance Manager GRC Site</u>	76
<u>Add Organizations</u>	76
Add an Organization	76
Move a Site to an Organization	78
<u>Create a New Site</u>	81
Compliance Manager GRC Manager GRC Dashboard	84

<u>Create Users and Assign Site Roles</u>	84
<u>Invite Users to Assessment Project</u>	89
<u>Set Up Report Settings</u>	93
Set Reports Text Preferences	95
Set Reports Logo Preferences	96
Set Themes Preferences	97
Set Reports Cover Images Preferences	99
Set Company Information Preferences	100
Use Network Detective to Add Your MSP Name to Report Headers	100
<u>Multi-sites View for Compliance Manager GRC</u>	102
Compliance Manager GRC Assessments	104
<u>Perform Rapid Baseline Assessment</u>	105
Select Standards and Controls	105
Step 1 — Select Standards	106
Step 2 — Select Controls	107
Add or Remove Individual Controls	111
Apply Custom Control Template	112
Step 3 — Continue Compliance Manager GRC Assessment	112
Begin Rapid Baseline Assessment	113
Customize Custom Policies and Procedures at the Site Level	120
Edit Requirement Policy and Guidance	120
Edit Control Guidance and Procedure Options	123
View Related Controls for Requirements	126
View Related Requirements for Controls	127
How Custom Requirements and Controls appear in Assessments	128
Import Site Standards and Controls	129
<u>Perform Controls Assessment</u>	132
Begin Controls Assessment	132
Import Baseline Responses	139
View Related Technical Issues	140
<u>Perform Requirements Assessment</u>	142
Begin Requirements Assessment	142

Introduction to Compliance Manager GRC

About Compliance Manager GRC: Governance, Risk & Compliance

Whether you've been asked to comply with federal and state laws, industry requirements, vendor contracts, cyber insurance policies or the forensic investigation following a breach, Compliance Manager GRC is here to simplify your life in performing all the required tasks.

Compliance Manager GRC Sweats the Details, So You Don't Have To

Compliance Manager GRC is purpose-built to automate compliance assessment, management and documentation tasks.

Here are just a few of the essential tasks that Compliance Manager GRC can handle for you:

- Get you started with a quick baseline risk assessment in less than an hour
- Automatically collect data on users, devices and networks for recurring assessments
- Generate dynamic Plans of Action & Milestones to address discovered issues
- Create customized policies and procedures manuals based on the way YOU do things
- Auto-consolidate the controls from all your different InfoSec requirements into a single operational controls document
- Show your progress against every standard or control set you're tracking
- Instantly produce evidence of compliance on demand
- Track employee compliance with training courses and policies
- Manage vendor risk assessments and compliance

A Customizable Compliance Solution

Compliance Manager GRC gives you the flexibility to manage multiple compliance standards and customized InfoSec programs, all at the same time and in the same place.

- Built-in Standards & Controls
- Build Your Own Standards
- Create Your Own Controls
- Manage Multiple Standards at the Same Time

Automated Reporting & Custom Documentation

Compliance Manager GRC automatically generates a dynamic set of evidence of compliance for every standard and security program you manage. All these reports, and more, can be easily regenerated based on the latest data:

- Customized Policies & Procedures
- Technical Assessment Report
- Technical Risk Analysis Report
- Technical Risk Treatment Plan
- Plan of Action & Milestones Report (POA&M)
- Auditor's Checklist
- Supporting Documents

Employee and Vendor IT GRC Tracking

A critical part of every cybersecurity program is tracking whether employees have read and acknowledged your policies, and whether they have taken your required cybersecurity training. Compliance Manager GRC includes a one-stop dashboard for managing Employee and Vendor compliance with these important non-technical requirements.

Compliance Manager GRC Assessment Overview

Compliance Assessment Overview

1. **Create a Compliance Manager GRC site** for the organization to be assessed
2. Select **Standards & Controls** to guide the compliance effort
3. Perform a quick **Rapid Baseline Assessment** to gain a high-level view of your compliance posture
4. **Collect data** from and conduct a **Technical Review** of the IT environment
5. **Establish evidence** for each control implemented with the **Controls Assessment**
 - Compliance Manager GRC has the ability to gather assessment information and then produce different reports specific to individual requirements. For example, a healthcare organization can print reports to show its implementation of the NIST Cybersecurity Framework (CSF) and then reports from the same data showing its compliance with HIPAA. Defense contractors can print reports showing their implementation of the current NIST 800-171 requirements and then reports showing how well prepared they are for CMMC.
7. Verify that all Standards requirements are met with the **Requirements Assessment**
 - The Requirements Assessment is similar to the Rapid Baseline Assessment, except that the questions asked are based on the Requirements of each selected standard. This ensures a maximum audit of how well your controls meet the requirements of your selected standard(s).
9. **Generate evidence of compliance** with customizable, automated reports

Available "Out-of-Box" Standards

In addition to allowing you to define your own custom compliance standards and controls, Compliance Manager GRC allows you to perform an assessment against the following "out-of-box" standards.

Note: New out-of-box standards are constantly being added! The list below may not include all currently available standards.

Currently available assessment standards	
• HIPAA	• GDPR-EU
• CMMC 2.0 Level 1 and 2	• GDPR-UK
• NIST CSF 2.0	• NIST 800-171
• NYS DFS Part 500 (Class A Companies, Covered Entities, and Small Businesses)	• NIST 800-171A
• Cyber Insurance Readiness	• Essential 8 (Maturity Level 1)
• UK Cyber Essentials (v3.1)	• CIS Controls v8
• PCI DSS (SAQ A, SAQ A-EP, SAQ B-IP, SAQ C, SAQ C-VT, SAQ D Merchant, SAQ D Service Provider)	• POPIA - Condition 7 - Security Safeguards
• FTC Safeguards Rule (Part 314)	• Kaseya Cybersecurity Fundamentals
• SOC 2 - Trust Services Criteria	



Network Prerequisites for Assessment Scans

For a successful network scan:

1. **ENSURE ALL NETWORK DEVICES 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 DEVICES.** See ["Pre-Scan Network Configuration Checklist" on page 401](#) 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 GRC will automatically suggest an IP range to scan on the network. However, you may wish to override this or exclude certain IP addresses.

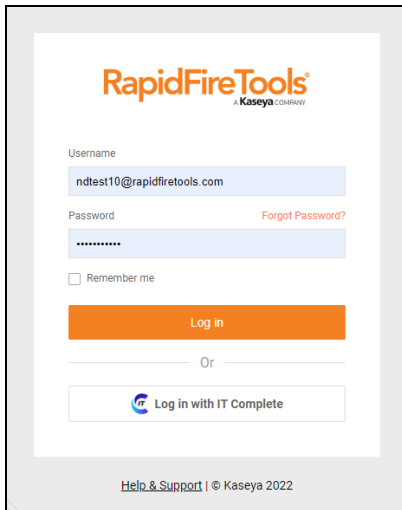
- **External IP addresses** for the organization to be used when setting up External Vulnerability Scans with the VulScan integration.
- **RapidFire Tools Portal User Credentials**
- For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IP address of the domain controller.
- For Windows Workgroup network environments, a list of the devices to be included in the Assessment and the Local Admin Credentials for each device.
- If using the Cloud Scan to assess a Microsoft Cloud environment, refer to the ["Prerequisites to Perform Cloud Scan using Enterprise App" on page 406](#).

Create a New Site

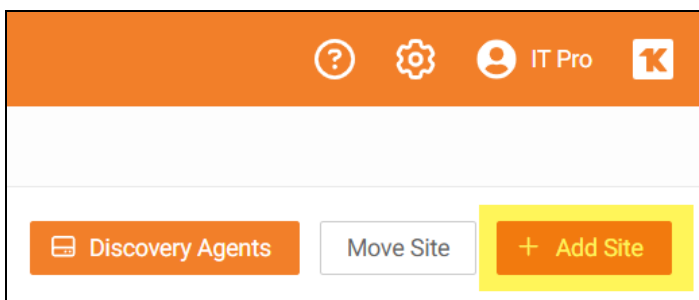
Tip: We recommend you get started by making a "practice site" and running your first assessment in-house. Use this to familiarize yourself with Compliance Manager GRC and the installation and configuration process.

The first step in performing a Compliance Manager GRC assessment is creating a "Site". Sites help you organize your assessments. This task is performed by a global admin user. To create a site:

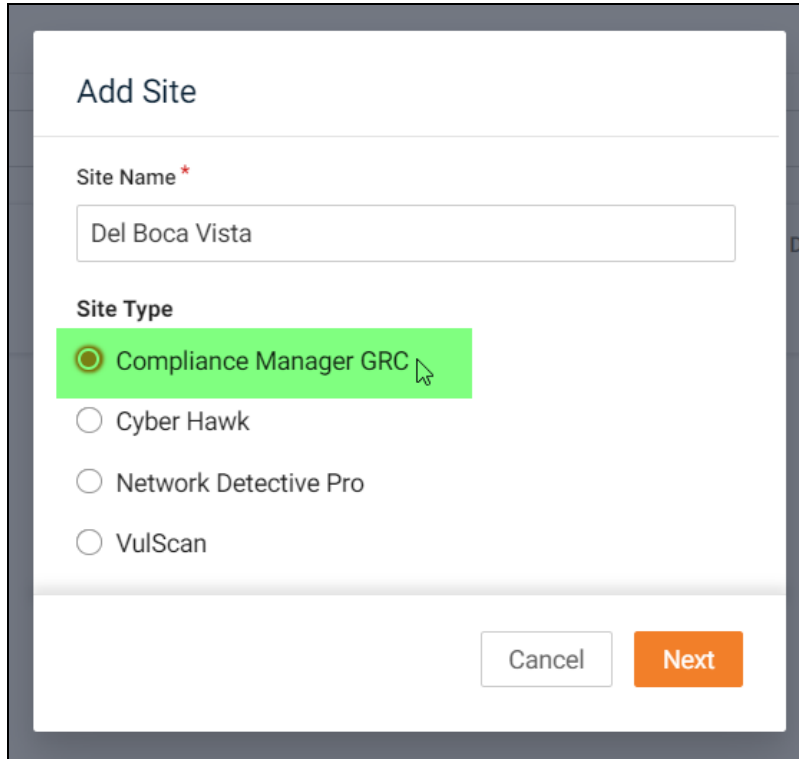
1. Access the RapidFire Tools Portal at <https://www.youritportal.com> and log in with your credentials.



2. Open an **Organization** or select **All Sites** from the left menu. Then, from the Sites page, click **Add Site**.

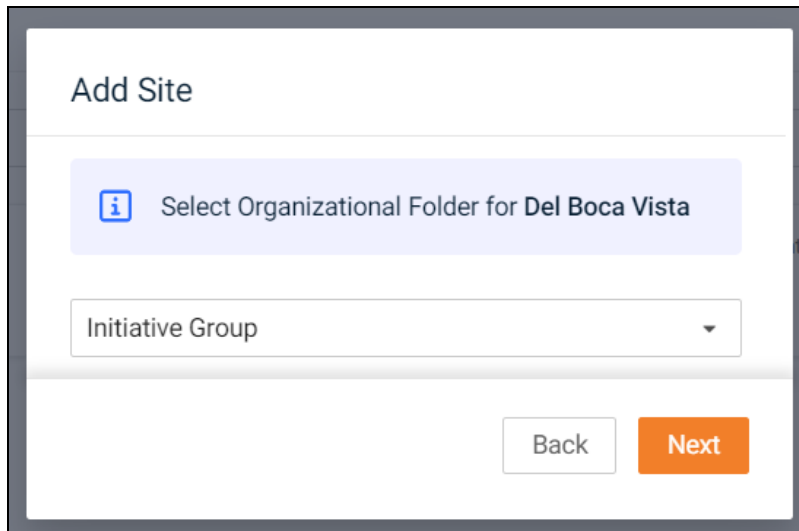


3. Enter a **Site Name**. For example, this can be the name of the company for whom the assessment is being performed.
4. Under **Site Type**, select **Compliance Manager GRC**.



The screenshot shows a web form titled "Add Site". It has two main sections. The first section, "Site Name", has a text input field containing "Del Boca Vista". The second section, "Site Type", has four radio button options: "Compliance Manager GRC" (which is selected and highlighted with a green background), "Cyber Hawk", "Network Detective Pro", and "VulScan". At the bottom right of the form are two buttons: "Cancel" and "Next".

5. Select an organizational folder for the new Compliance Manager GRC site.

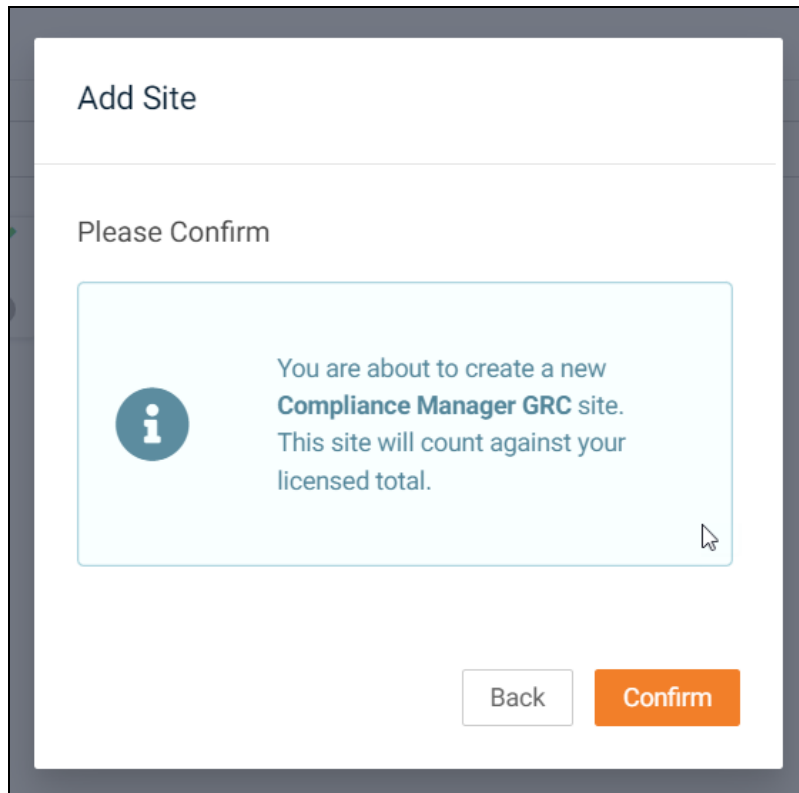


The screenshot shows the same "Add Site" form, but now it has a light blue instruction box that says "Select Organizational Folder for Del Boca Vista" with an information icon. Below this is a dropdown menu currently showing "Initiative Group". The "Back" and "Next" buttons are still at the bottom right.

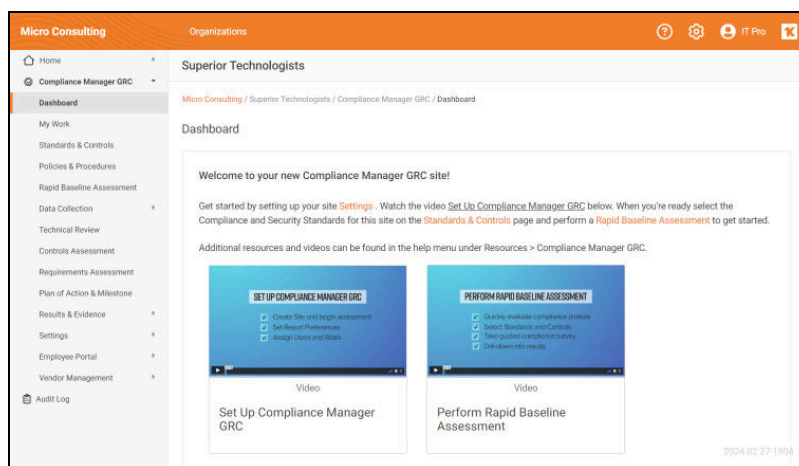
6. Confirm that you wish to create the site.

Note: Note that this will involve using one of your available Compliance Manager GRC licenses. RapidFire Tools products employ various licensing

models appropriate for the scale of your IT assessment needs. Contact your account manager for specific questions regarding your available licenses.

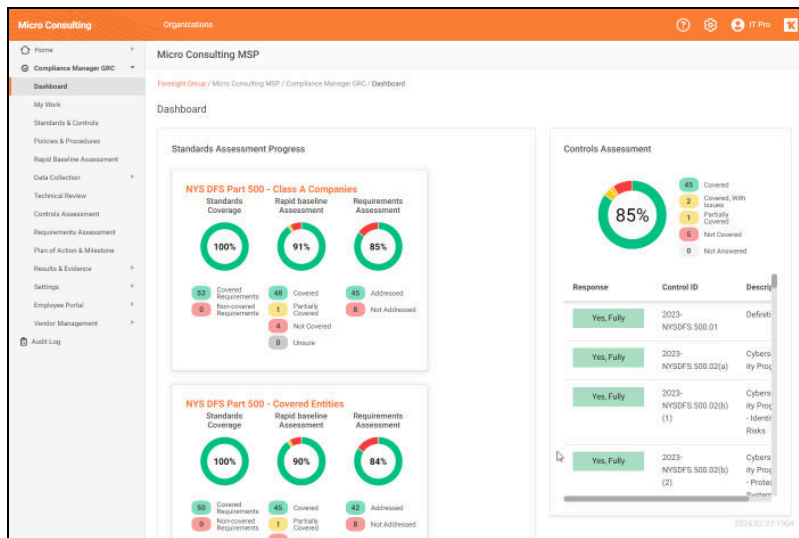


7. When you create the site, you will land at the site dashboard. From here you can begin managing compliance efforts for your site. See ["Perform Rapid Baseline Assessment" on page 105](#).



Compliance Manager GRC Manager GRC Dashboard

When you finish your first Rapid Baseline Assessment, the **Compliance Manager GRC dashboard** will display the results of your audit. From the dashboard you can quickly review the status of your assessments. You can also click on the radial graphs to access your Standards and Controls, as well as the Rapid Baseline Assessment, Controls Assessment, and Requirements Assessment.



Create Users and Assign Site Roles

Before you begin your assessment, you can optionally create additional Users and assign them site Roles. Assign Roles to enlist users in performing different parts of the assessment, such as data collection or completing assessment worksheets. Further, Roles ensure users can access only those areas of the site that are necessary to perform their tasks.

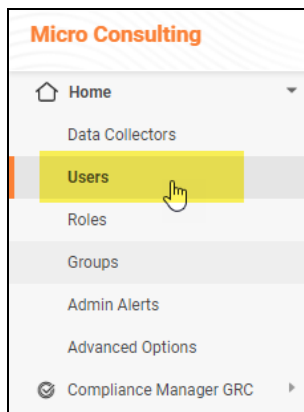
Here's a high-level breakdown of site access for each Role:

- **Site Admin:** Can access all site functionality
- **Internal Auditor:** Can access assessments, but not data collection or users
- **Technician:** Can access assessments and data collection, but not users
- **SME:** Can only access invited worksheets and assigned questions
- **Reports Viewer:** Can only access Results & Evidence and Reports (see ["Create Reports Viewer User" on page 338](#))
- **Employee Portal Admin:** Can only access and manage Employee Portal (see ["Employee Portal " on page 351](#))

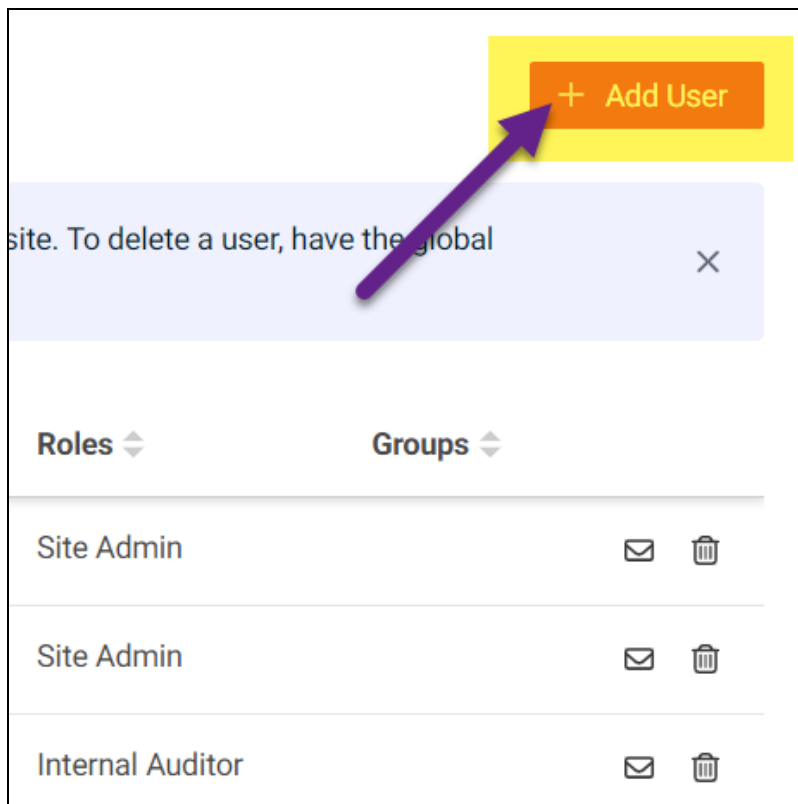
Note: You can find a complete breakdown of site Roles here: ["Compliance Manager GRC Site Access by Roles" on page 475](#).

Here's how to create Users and assign them project Roles:

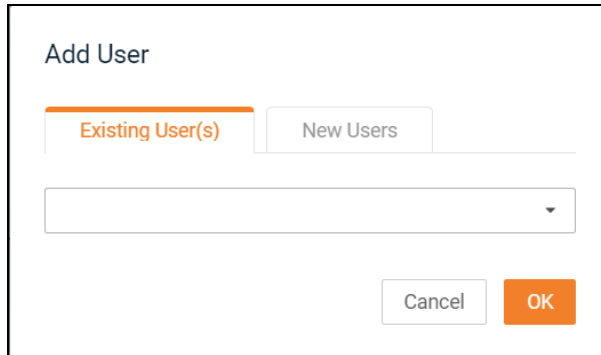
1. From the Home page for your Site, click **Users**.



2. Click **Add User**.



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



The screenshot shows a modal window titled "Add User". It contains two tabs: "Existing User(s)" which is currently selected and highlighted with an orange border, and "New Users". Below the tabs is a text input field with a small downward arrow on the right side, indicating it's a dropdown menu. At the bottom right of the modal are two buttons: "Cancel" and "OK".

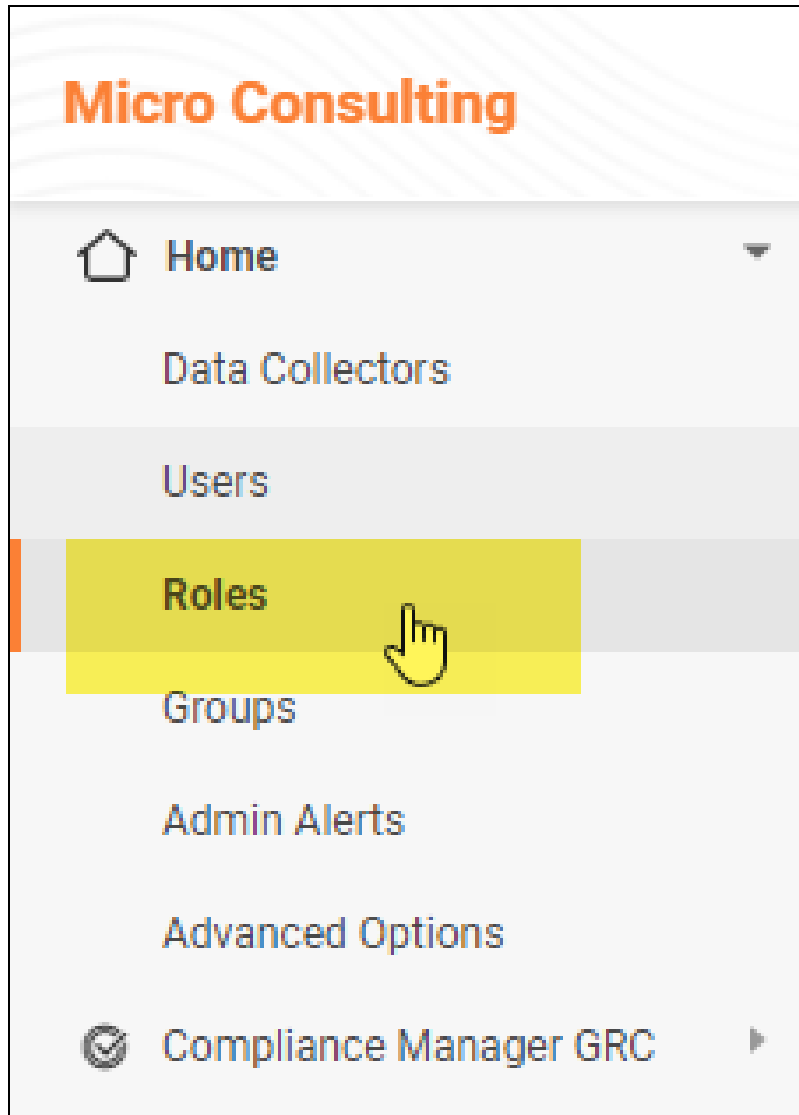
- ii. Alternatively, you can create a **New User** account to provide individuals access to the Portal and assessment process. You will need to enter an email address, first and last name, and password for each user.

Note: Send new users their login credentials after you add them to the site. You can also ["Invite Users to Assessment Project" on page 89](#).

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

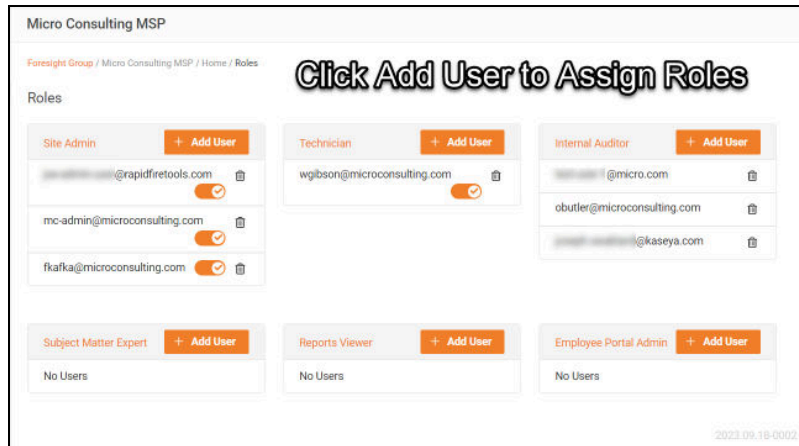
Next you will associate these new users with your Compliance Manager GRC Site. To do this:

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



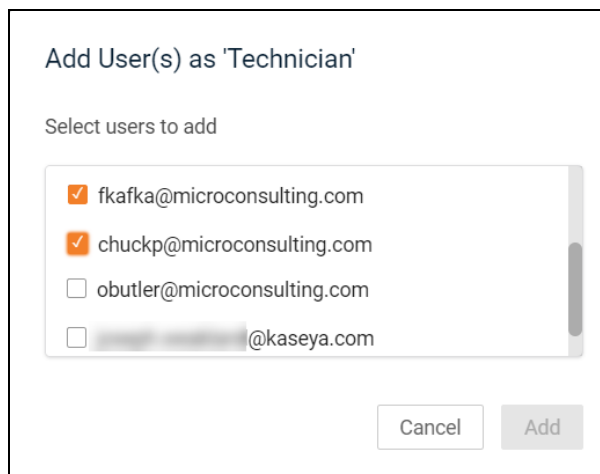
4. Next to each role, click **Add User** to assign users to desired roles.

Note: For the Site Admin and Technician Role, activate the slider to enable user access to organization-level Discovery Agents. See also ["Enable Organization Discovery Agents \(Compliance Manager GRC\) for Local Data Collection" on page 202](#).



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.



6. When you have finished adding users to your site and assigning roles, you can continue your Compliance Manager GRC assessment.

Perform Technical Review

The **Technical Review** combines automated data collection with guided input to identify technical issues and provide evidence of compliance. When you begin the Technical Review, a series of worksheets will be created based on the scan data you collected for the site. This section of the guide outlines how to perform the Technical Review from start to finish.

<u>Begin Technical Review and Generate Worksheets</u>	250
Step 1 — Verify Data Collection for Site	250
Step 2 — Begin Technical Review and Generate Worksheets	250
Step 3 — Open and Complete all Worksheets	253
<u>Complete Technical Review Worksheets</u>	254
Application Inventory Worksheet	255
Asset Inventory Worksheet	256
Enterprise Application Inventory Worksheet	257
External Information Systems Worksheet	258
External Port Use Worksheet	259
File Share Identification Worksheet	260
Local Computer User Access Review Worksheet	260
Sensitive Data Assessment Worksheet	262
System Information Worksheet	263
User Access Review Worksheet	264
<u>Invite Subject Matter Experts (SMEs) to Complete Technical Review Worksheets</u>	266
<u>Manage Worksheet Invites for SMEs</u>	269
<u>Tips for Completing Technical Review Worksheets</u>	272
Attach Supporting Documents	274
Add Respondent	275
Copy and Paste Responses (Bulk Update)	276

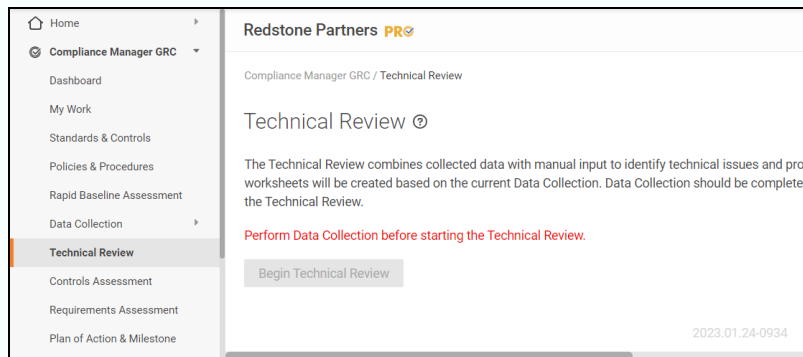
Begin Technical Review and Generate Worksheets

During the Technical review, you will collect and enter information about the site that cannot be discovered solely through automated scans. Follow these steps to perform the Technical Review:

Step 1 — Verify Data Collection for Site

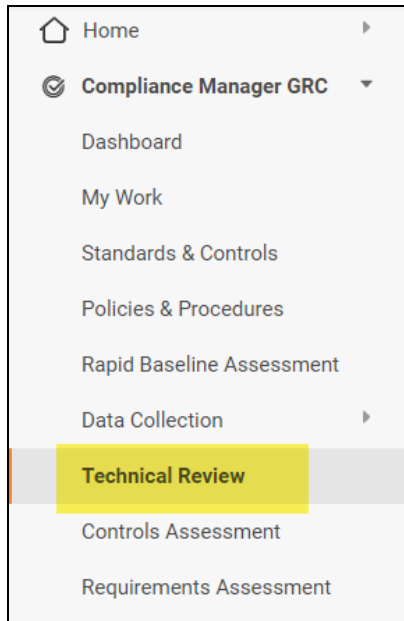
Data collection should be complete to largest extent possible before beginning the Technical Review. At a minimum, you must perform a LAN Scan. We also recommend that you perform Local Computer Scans on devices that could not be reached during the LAN Scan. This will generate scan data that forms a representative sample — if not a complete sample — of devices in the assessment environment. See ["Perform Technical Review Assessment Scans" on page 173](#).

Note: You cannot perform the Technical Review before you collect data for the site.

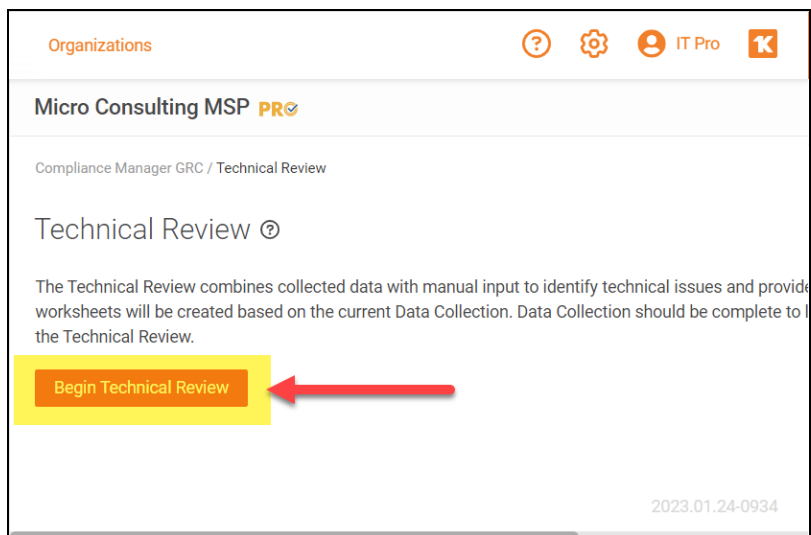


Step 2 — Begin Technical Review and Generate Worksheets

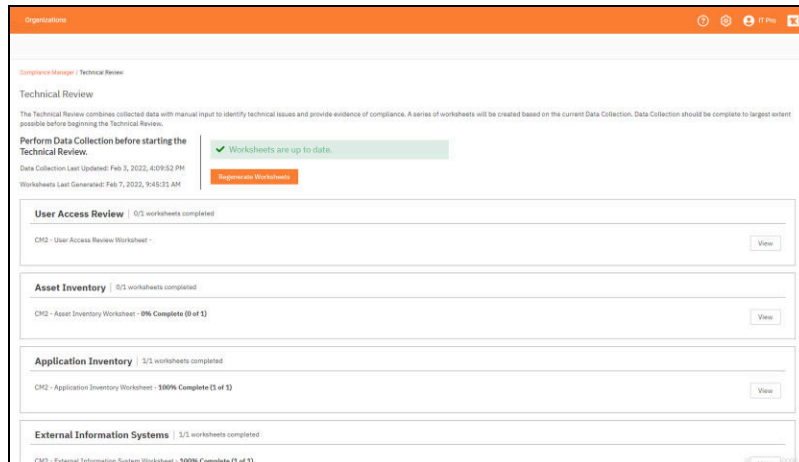
1. Once you collect data for your site, navigate to **[Your Site] > Compliance Manager GRC > Technical Review**.



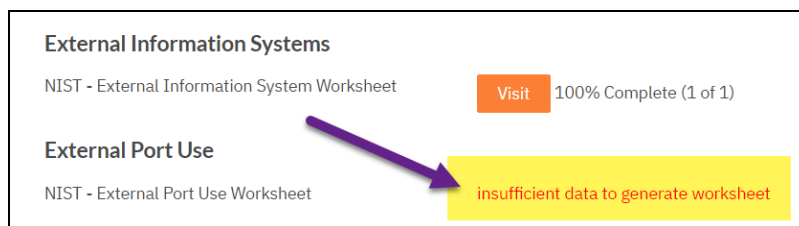
2. Click **Begin Technical Review**.



3. After a moment, the assessment worksheets will appear.



- Worksheets may be unavailable if you did not perform all of the prerequisite scans. For example, if you did not import an external vulnerability scan from a VulScan site, that worksheet will not be available.

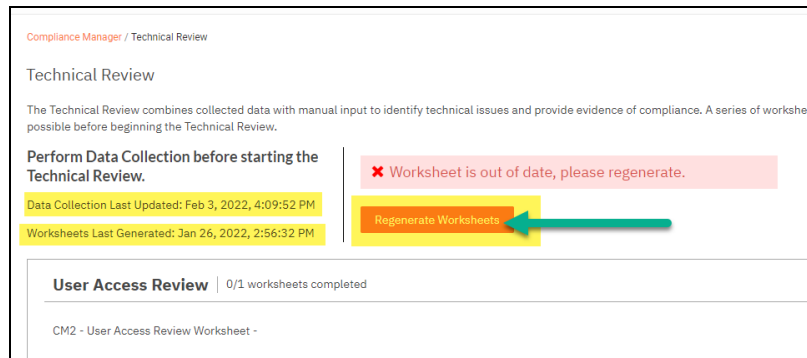


Regenerate Worksheets

If new scan data becomes available for your site, you must regenerate the worksheets with the latest results. If prompted, click **Regenerate Worksheets**. In a moment, your new worksheets will appear.

Note: From the Technical Review page, you can see the date/time of your most recent data collection, as well as the date/time when the latest worksheets were generated.

Note: Previously saved data will remain in the updated worksheet; your progress will not be lost.



Compliance Manager / Technical Review

Technical Review

The Technical Review combines collected data with manual input to identify technical issues and provide evidence of compliance. A series of worksheets are generated and updated as new data is collected, so it is important to regenerate the worksheets as soon as possible before beginning the Technical Review.

Perform Data Collection before starting the Technical Review.

Data Collection Last Updated: Feb 3, 2022, 4:09:52 PM

Worksheets Last Generated: Jan 26, 2022, 2:56:32 PM

✖ Worksheet is out of date, please regenerate.

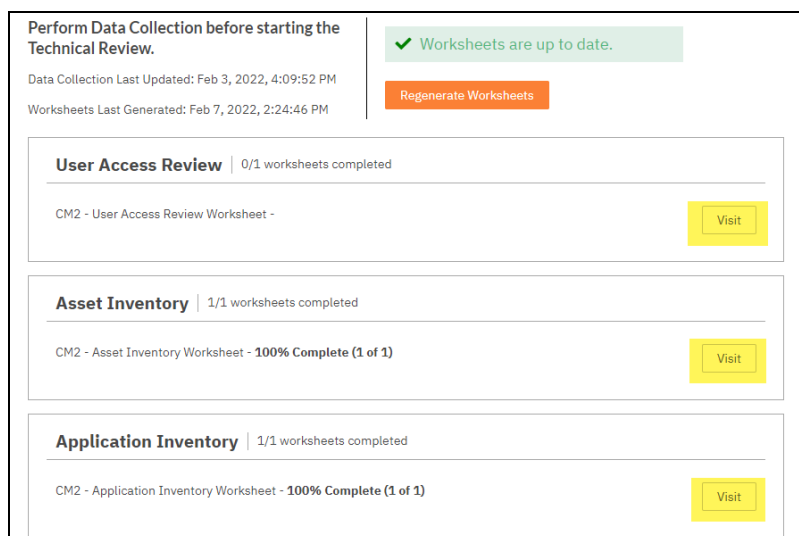
Regenerate Worksheets

User Access Review | 0/1 worksheets completed

CM2 - User Access Review Worksheet -

Step 3 — Open and Complete all Worksheets

1. Once the worksheets appear, click **View** to open a worksheet.



Perform Data Collection before starting the Technical Review.

Data Collection Last Updated: Feb 3, 2022, 4:09:52 PM

Worksheets Last Generated: Feb 7, 2022, 2:24:46 PM

✔ Worksheets are up to date.

Regenerate Worksheets

User Access Review | 0/1 worksheets completed

CM2 - User Access Review Worksheet - **Visit**

Asset Inventory | 1/1 worksheets completed

CM2 - Asset Inventory Worksheet - **100% Complete (1 of 1)** **Visit**

Application Inventory | 1/1 worksheets completed

CM2 - Application Inventory Worksheet - **100% Complete (1 of 1)** **Visit**

2. You will then enter the required data into the worksheet. See ["Complete Technical Review Worksheets" on the facing page](#) and ["Tips for Completing Technical Review"](#)

Tips for Completing Technical Review Worksheets

During the Technical Review, you will use worksheets to collect information about the site that cannot be discovered solely through automated scans. This section details some helpful instructions and time-saving tips that you can use to breeze through your assessment documentation.

EXAMPLE:

To complete a Technical Review worksheet, follow these steps:

- i. Review the *Topic* (i.e. the specific field or question within the form).

The screenshot shows a worksheet titled 'PERFORMANCEIT.COM'. It has a green checkmark icon and a 'Download' button. Below the title, there's a section for '1.1 File Share Authorization' with instructions: 'Indicate if the network share is authorized to store sensitive data.' Below the instructions is a table with columns: Share, Location, Storage Authorization, and Source. The table contains three rows of data. Red arrows point to the 'Section' (PERFORMANCEIT.COM), 'Topic/Question' (1.1 File Share Authorization), 'Instructions' (Indicate if the network share is authorized to store sensitive data), and 'Response field' (Storage Authorization dropdown menu).

Share	Location	Storage Authorization	Source
\\DC01\NETLOGON	C:\Windows\SYSVOL\sysvol\test performancet.com\SCRIPTS	Not Authorized	On-Prem
\\DC01\SYSVOL	C:\Windows\SYSVOL\sysvol	Not Authorized	On-Prem
\\DC02\NETLOGON	C:\Windows\SYSVOL\sysvol\test performancet.com\SCRIPTS	Not Authorized	On-Prem

- ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.
- iii. Enter the *Response*. For most Technical Review worksheets, you will select an option from a drop-down menu for each worksheet entry.

The screenshot shows a table with columns: User Name, Display Name, Privileged (Administrator) Account, Last Login, Account Type, Is This Account Authorized?, and Source. The table contains several rows of data. A red arrow points to the 'Account Type' dropdown menu, which is currently set to 'Former User'.

User Name	Display Name	Privileged (Administrator) Account	Last Login	Account Type	Is This Account Authorized?	Source
Administrator	Administrator	Yes	30-May-2023 4:28:43 AM	Former User	No	On-Prem AD
Administrator	Administrator	Yes	10-May-2023 12:37:12 AM	Current User	No	On-Prem AD
Administrator	Administrator	Yes	10-May-2023 12:37:12 AM	Current Third Party	No	On-Prem AD
Administrator	Administrator	No	16-Feb-2023 9:48:25 PM	Former User	No	On-Prem AD
Administrator	Administrator	Yes	16-Feb-2023 9:48:25 PM	Former Third Party	No	On-Prem AD
Administrator	Administrator	No		Service Account	No	On-Prem AD
Administrator	Administrator	No		System Account	No	On-Prem AD
Administrator	Administrator	No		Current Third Party	No	On-Prem AD

When you complete a section of the worksheet, a **green check mark** indicator will appear.

1

PERFORMANCEIT.COM

Section complete

1.1 User Access Review

The table below lists the users discovered on the network. For each user, specify the account type. Then classification.

Previous Assessment Response: Multiple Responses

[View Previous Responses](#)

User Name	Display Name	Privileged (Administrator) Account	Last Login
		Yes	30-May-2023 4:28:43 AM
		Yes	

iv. **Save** frequently. When you are done, click **Save and Return**.

Former User	No	On-Prem AD
Current Third Party	No	On-Prem AD

Save

Save and Return

Return

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 GRC. To attach a supporting document:

1. Scroll down to the bottom of the worksheet entries for a section. Click **Add Attachments**.

			AM
mwadmin	M Wu	Yes	
mjones	Marley Jones	No	12-Mar-2019 10:45:56 AM
maryia.tulai	Maryia Tulai	No	17-Feb-2023 1:34:43 AM
mptest	MP Test	No	01-Feb-2019 10:31:31 AM

Add Notes
Add Respondent
Add Attachments

2. Choose whether to Add Attachment from **Previously Uploaded** or from your **Local Computer**. You can also ["Attach IT Glue documents for Worksheets" on page 429](#).

Add Notes
Add Respondent
Add Attachments

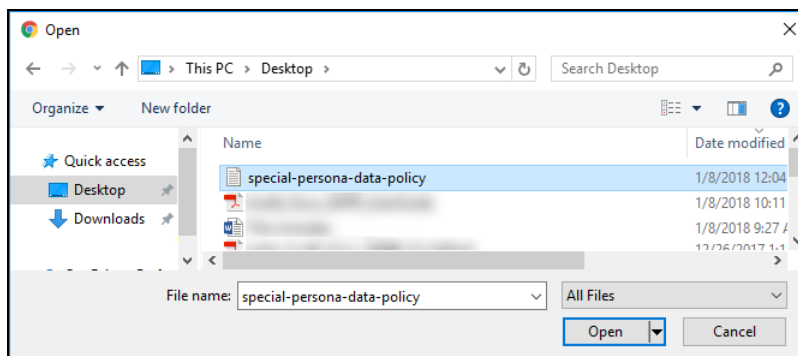
Attachments:

File Name Upload Date

Add Attachment:
From Previously Uploaded
Upload Local File
From IT Glue

Hide

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.

File Name	Upload Date	Uploaded By
Baseline_Configuration_Policy.pdf	May 2, 2023, 12:01:17 PM	@rapidfiretools.com

Add Attachment:

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

Add Respondent

You can add a **Respondent** to enter the name of individual that provided information for a worksheet. To add a respondent:

- Scroll down to the bottom of the worksheet entries for a section. Click **Add Respondent**.

		No	
		No	
		No	04-May-2023 8:28:20 AM
		Yes	16-Feb-2023 9:08:21 AM

- Enter the **Respondent name**. The name will be appended to the responses when your assessment documentation is generated.

henry.homiller	Henry Homiller	No	04-May-2023 8:28:20 AM
isadmin	Ina Schmidt	Yes	16-Feb-2023 9:08:21 AM

Respondent:
Micro Professional

Copy and Paste Responses (Bulk Update)

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 with a bulk entry. 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.

	Account Type	Is this Account Authorized?	Source
10:46:12	Former User	No	On-Prem AD
12:01:11	Current User	No	On-Prem AD
12:52:07	Current Third Party	No	On-Prem AD
12:00:45	Former User	No	On-Prem AD
	Former Third Party	No	On-Prem AD
	Service Account	No	On-Prem AD

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

	Account Type	Is this Account Authorized?	Source
12:12	Former User	No	On-Prem AD
11:11	Former User	No	On-Prem AD
7:07	Former User	No	On-Prem AD
10:45	Current Third Party	No	On-Prem AD
	Current Third Party	Yes	On-Prem AD

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.

	Account Type	Is this Account Authorized?	Source
1:31	Former User ▼	No ▼	On-Prem AD
1:17	Former User ▼	Yes ▼	On-Prem AD
3:25	Former User ▼	No ▼	On-Prem AD
42	Former User ▼	No ▼	On-Prem AD
1:01	Former User ▼	No ▼	On-Prem AD

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

Policies and Procedures

With Compliance Manager GRC, you can generate **Policies & Procedures** based on the Standard(s) and/or Controls assigned to your assessment sites. These documents can be used as evidence of compliance and to guide the implementation of site security controls. Select your standards and controls, and print a customized set of policies ready to get approved and shared.

Note: Your policies and procedures can be customized according to your exact requirements. See ["Customize Custom Policies and Procedures at the Site Level" on page 120](#). See also ["Manage Standards and Controls" on page 380](#) to create custom standards and controls at the global level. Your custom policies and procedures will appear in the documents you generate.

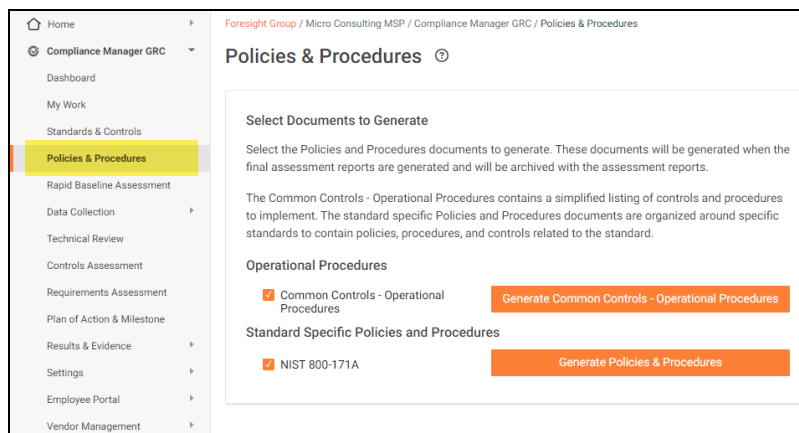
In this topic, you can find:

- ["Generate Policies & Procedures" below](#)
- ["Generate Common Controls — Operational Procedures" on the next page](#)
- ["Expanded Policies and Procedures Templates" on page 281](#)

Generate Policies & Procedures

To generate policies and procedures for your chosen standards:

1. From your Site, navigate to **Compliance Manager GRC > Policies & Procedures**.



Note: You must have at least one standard and one control selected in order to generate Policies & Procedures.

2. From **Standard Specific Policies and Procedures**, click the **check-box** to select the standard.
3. Then click **Generate Policies & Procedures** for the standard.

Policies & Procedures ⓘ

Select Documents to Generate

Select the Policies and Procedures documents to generate. These documents will be generated when the final assessment reports are generated and will be archived with the assessment reports.

The Common Controls - Operational Procedures contains a simplified listing of controls and procedures to implement. The standard specific Policies and Procedures documents are organized around specific standards to contain policies, procedures, and controls related to the standard.

Operational Procedures

☐ Common Controls - Operational Procedures Generate Common Controls - Operational Procedures

Standard Specific Policies and Procedures

☒ NIST 800-171A Generate Policies & Procedures

Note: It may take several seconds for your policy document to appear as a .docx download.

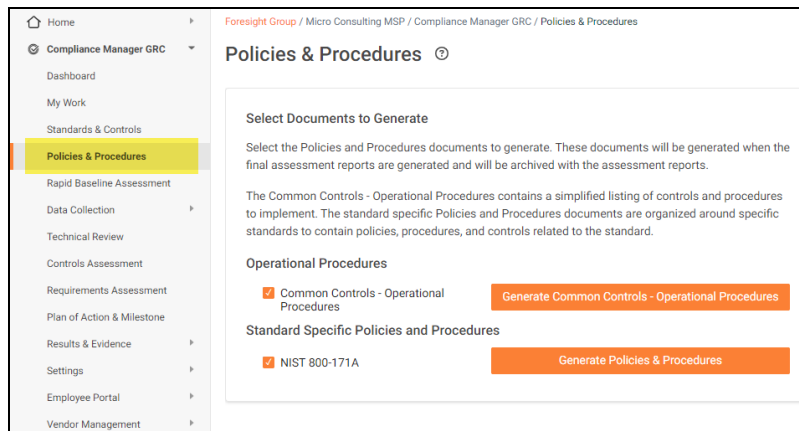
The generated document will detail procedures based on the selected standards and controls. With the check-box for the standard selected, the document will also appear in your assessment documentation when you ["Generate Reports" on page 306](#).

Generate Common Controls — Operational Procedures

While you can generate policy documents based on selected standards, you can also generate an **Operational Procedures** document that details all controls in place at the site. Because the Operational Procedures cover all controls, it can provide your tech team with a single implementation "play book."

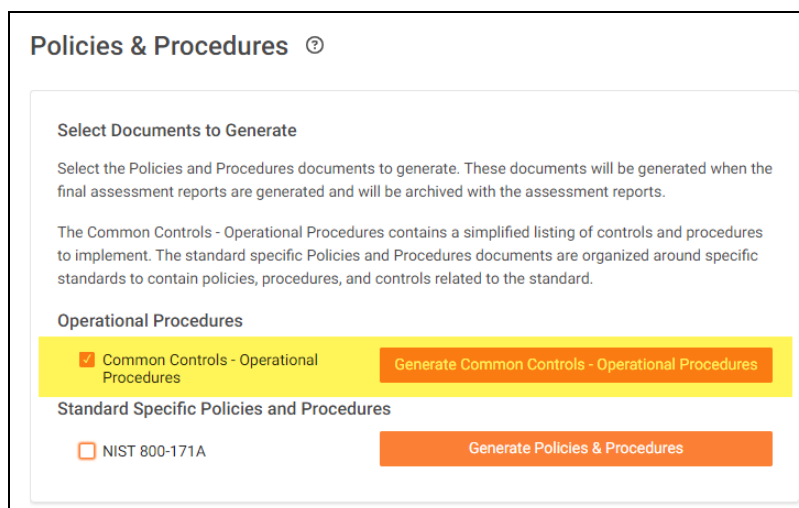
To do this:

1. From your Site, navigate to **Compliance Manager GRC > Policies & Procedures**.



Note: You must have at least one standard and one control selected in order to generate Operational Procedures.

2. From Operational Procedures, click the **check-box** to select **Common Controls — Operational Procedures**
3. Then click **Generate Common Controls — Operational Procedures**.



Note: It may take several seconds for your policy document to appear as a .docx download.

Note: The generated document will detail procedures based on the selected standards and controls. These appear under the "Procedures" subheading for

each Control.

The screenshot shows a document titled "Operational Procedures COMMON CONTROLS" with a sub-header "CC1.1 - Inventories". The document is structured as follows:

Requirements	Other Requirements
NIST CSF: ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4	- HIPAA - Security Rule: 164.308(a)(1)(ii)(A) - EU GDPR - Controller and Processor: Article 24(1) - UK GDPR - Controller and Processor: Article 24(1)

Description
Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

Guidance
Automatically or manually identify and locate all hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware. Create reports and update as required.

Procedure

- Use automated tools to identify, locate, and document all PCs, laptops, and servers, including virtual and cloud-based platforms, and identify what data is stored on each.
- Use manual methods, including interviewing users, to identify and locate all PCs, laptops, servers, mobile devices, portable media, cloud services, network devices, printers, and other network-enabled devices, and identify what data is stored on each.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Sanctions/Compliance
Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

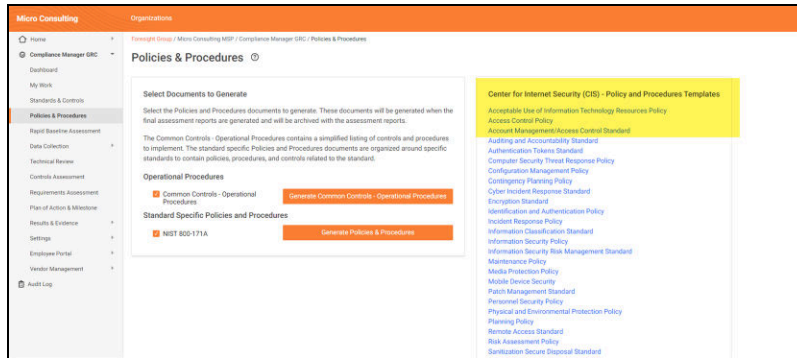
With the check-box for the Common Controls selected, the selected document will also appear in your assessment documentation when you ["Generate Reports" on page 306](#).

Expanded Policies and Procedures Templates

From Policies & Procedures, in addition to generating procedure documents based on your selected compliance standards, you can also access a list of sample IT Security policy templates for download and use. These cybersecurity policies and procedures are based on guidance from the Center for Internet Security (CIS) (www.cisecurity.org).

The available templates cover a broad range of cybersecurity best practices. They can further save time when creating custom IT Security policies documents for use by an organization.

You can access this expanded array of Policies and Procedures Templates under **Center for Internet Security (CIS) - Policy and Procedures Templates**.



To access a template, click on it to download it. The document will then be available for you to customize for your intended purpose and the target organization.

Policy #:	Title:	Effective Date:
X.XXX	Access Control Policy	MM/DD/YY

PURPOSE

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164; NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of [entity] resources and assets.

1. ACCOUNT MANAGEMENT
IT Department shall:
 - a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency,

You can find a complete list of the available CIS Policies and Procedures Templates below:

- Acceptable Use of Information Technology Resources Policy
- Access Control Policy
- Account Management/Access Control Standard
- Auditing and Accountability Standard
- Authentication Tokens Standard
- Computer Security Threat Response Policy
- Configuration Management Policy
- Contingency Planning Policy

- Cyber Incident Response Standard
- Encryption Standard
- Identification and Authentication Policy
- Incident Response Policy
- Information Classification Standard
- Information Security Policy
- Information Security Risk Management Standard
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Planning Policy
- Remote Access Standard
- Risk Assessment Policy
- Sanitization Secure Disposal Standard
- Secure Coding Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard
- Security Assessment and Authorization Policy
- Security Awareness and Training Policy
- Security Logging Standard
- System and Communications Protection Policy
- System and Information Integrity Policy
- Systems and Services Acquisition Policy
- Vulnerability Scanning Standard
- 802.11 Wireless Network Security Standard