PRESIDIO

NGRM CYBER SECURITY

USER GUIDE

Version 2.1

May 15, 2019

Table of Contents

NGRM Cyber Security Portal is a job aid for Presidio Security Practice professionals and customers that helps them visualize, work through, and track security issues found during Presidio NGRM engagements.

1. Accounts & Roles

Depending on the job role assigned to your account, you will have varying degrees of access to view, create or modify, and manage findings. This role-based access system allows Administrators and Customers to securely control data while having the right amount of visibility into security issues.

1.1. Role-based access

There are three roles available listed here from least to most access:

1.1.1. Customer

Customer users have access to the dashboard, and view-only access to risks, vulnerabilities, governance, compliance and resources. They also only have access to their own user accounts.

1.1.2. Manager

Manager users have access to the dashboard, and limited editing abilities to risks, vulnerabilities, governance, compliance and resources. They have access to their own user accounts, and those of any customer user in their company.

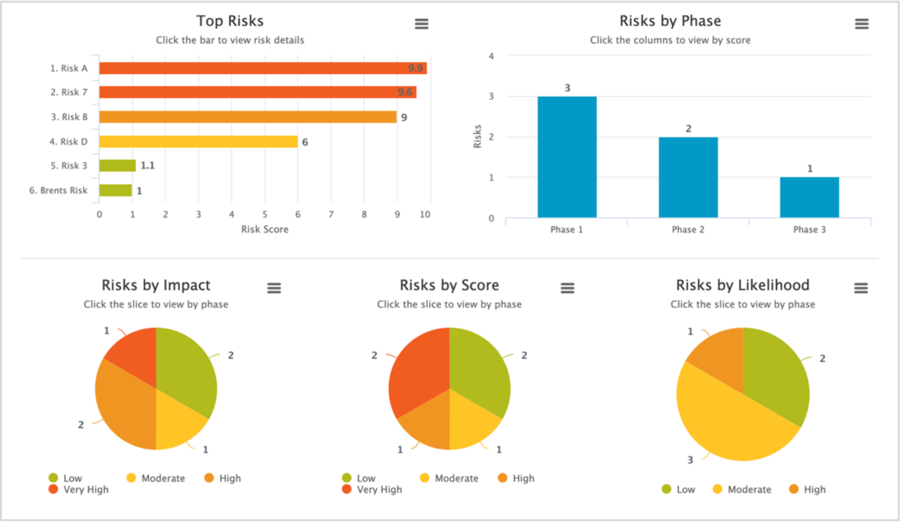
1.1.3. Admin

Admin users have full editing access to all aspects of NGRM use, including risks, vulnerabilities, resources and user accounts. Admins are responsible for uploading security assessment data, reports, and onboarding users.

2. Data Visualization Components

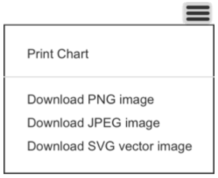
2.1. Interactive Charts

Charts can be used to drill down into greater detail. On most charts, you can click on the bars of bar charts or pie sections of pie charts to dynamically view the next level of detail/information. You can also click the chart legend values to toggle them on and off in the chart. The tables under these charts dynamically update their filters based on what you click to filter in the charts.



2.1.1. Export Menu

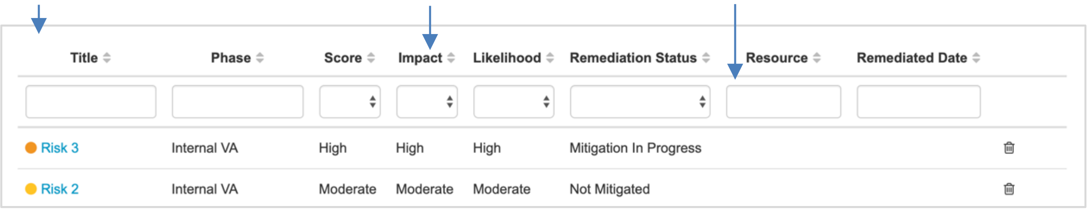
To download or print any chart, click the hamburger menu icon located in the upper right corner of the chart to display the export options.



2.2. Dynamic Data Tables

At the top of each table, just under the column headers, there are text boxes or drop down lists that dynamically filter the table as you enter text or select items from the drop down list. The filters will be auto-populated and the data table will be dynamically updated based on selections made on the charts above. You can change the table sorting from ascending to descending by clicking the column header by which you want to sort.

Table **Column Header** **Filter**



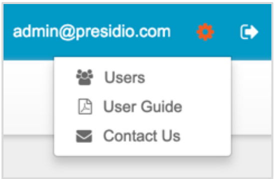
Title ⇕	Phase ⇕	Score ⇕	Impact ⇕	Likelihood ⇕	Remediation Status ⇕	Resource ⇕	Remediated Date ⇕	
		⇕	⇕	⇕	⇕			
● Risk 3	Internal VA	High	High	High	Mitigation In Progress			🗑
● Risk 2	Internal VA	Moderate	Moderate	Moderate	Not Mitigated			🗑

3. Header Components

3.1. App Bar

3.1.1. Settings Cog Icon

The settings cog icon in the top navigation App Bar (highlighted in orange) gives you access to user account information, a link to this User Guide, and a link to contact Presidio Cyber Support if you need assistance. Clicking Contact Us will create an email that is populated with the support email alias.

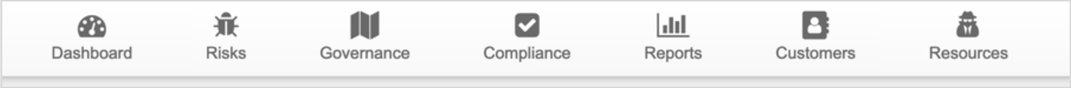


3.1.2. Logout Icon

Clicking this icon logs you out of the portal.

3.2. Main Menu

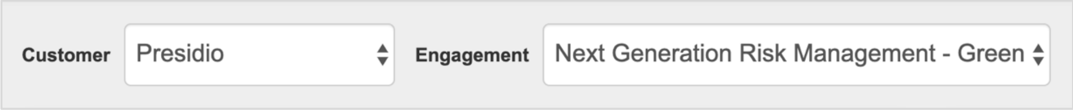
Residing beneath the App Bar, the Main Menu is also sticky to the top of the browser and links all users to the main sections of NGRM. Refer to section 1.1 for role-based menu options.



3.3. Customer & Engagement Selectors

The Customer drop-down list is only useful for Admins who are able to access more than one customer's data. Manager and Customer users can only see their own customer name in this list.

If a customer has more than one engagement active in the system, users can view data for each by selecting an engagement from this drop-down list.

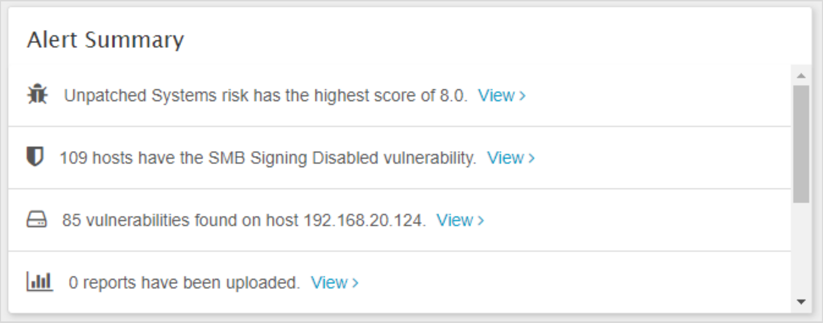


Customer Presidio **Engagement** Next Generation Risk Management - Green

4. Dashboard Components

4.1. Alert Summary

The Alert Summary lists the Risk with the highest score, the Vulnerability affecting the most Hosts, and the Host with the most total Vulnerabilities, and provides a quick view of the latest activities across the portal. Clicking the View › link takes you to the section of NGRM from where the alert was generated.



Alert Summary

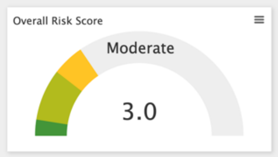
Unpatched Systems risk has the highest score of 8.0. View ›

109 hosts have the SMB Signing Disabled vulnerability. View ›

85 vulnerabilities found on host 192.168.20.124. View ›

0 reports have been uploaded. View ›

4.2. Overall Risk Score Chart

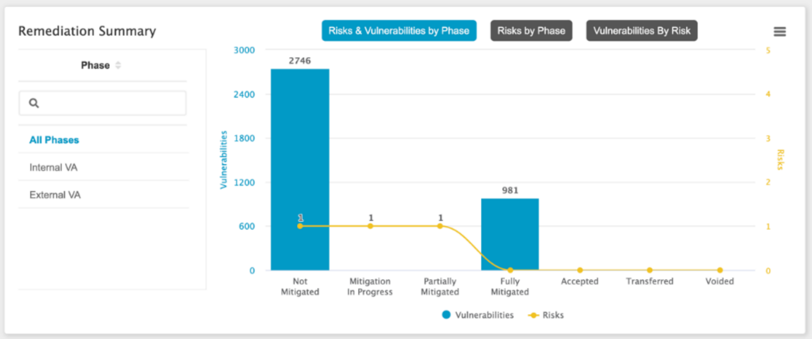


The Overall Risk Score chart graphically displays your overall risk score for the selected engagement as determined by the security assessment across risks, governance and compliance.

4.3. Remediation Summary Chart

This chart combines several components to provide a high-level view into the Remediation Status for Risks and Vulnerabilities. The blue and grey buttons above the main chart area allow you to toggle between three views of the chart. Each chart has options on the left hand side that allows you to filter by Phases or Risks.

- Risks and Vulnerabilities by Phase is the default view. It displays the count of both Risks and Vulnerabilities for each Remediation Status. The chart can be filtered by phase.
- Risk by Phase displays the risks status and includes the Risk Score category. The chart can be filtered by phase.
- Vulnerabilities by Risk displays the vulnerability status and includes the Risk Score category. The chart can be filtered by Risk.

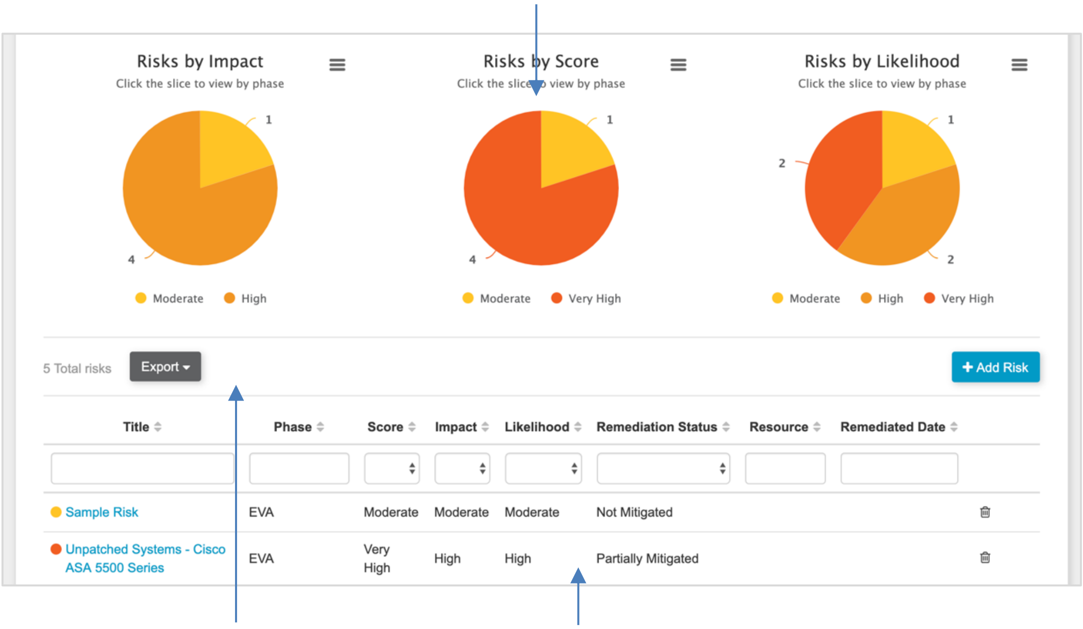


5. Risks, Hosts, and Vulnerabilities

Clicking the Risks icon in the Main Menu will display the Risks section that defaults to the Risks tab. Other tabs available within this section are Vulnerabilities and Hosts. Each of these tabs represents a different way to view the risks identified during your security assessment.

The layout for each page is consistent and includes Charts at the top followed by the Export/Import Bar and the Data Table at the bottom of the page.

Interactive Charts


Risks by Impact
Click the slice to view by phase
1
4
● Moderate ● High
Risks by Score
Click the slice to view by phase
1
4
● Moderate ● Very High
Risks by Likelihood
Click the slice to view by phase
1
2
2
● Moderate ● High ● Very High
5 Total risks
Export ▾
+ Add Risk

Title	Phase	Score	Impact	Likelihood	Remediation Status	Resource	Remediated Date	
● Sample Risk	EVA	Moderate	Moderate	Moderate	Not Mitigated			🗑
● Unpatched Systems - Cisco ASA 5500 Series	EVA	Very High	High	High	Partially Mitigated			🗑

Export/Import Bar **Data Table**

5.1. Interactive Charts

5.1.1. Risk Charts

Your identified Risks are presented using different charts:

- Top Risks shows your Risks broken down by Risk score, from highest to lowest. Clicking on the bar filters the table below to only show those risks that match the bar you clicked.
- Risks by Phase shows you the breakdown of your Risks by their associated Phase. Clicking on a bar filters the table below to only show those risks that match the phase you clicked.
- Risks by Impact shows you the breakdown of your risks by their impact. Clicking on the pie slices drills down to show the phase(s) of the risks with the impact value you clicked. It also filters the table below to only show those risks that match the impact level you clicked.

- Risks by Score shows you the breakdown of your risks by their score. Clicking on the pie slices drills down to show the Phase(s) of the Risks with the score value you clicked. It also filters the table below to only show those risks that match the score you clicked.

- Risks by Likelihood shows you the breakdown of your risks by the likelihood of someone trying to exploit the risk. Clicking on the pie slices drills down to show the phase(s) of the risks with the likelihood value you clicked. It also filters the table below to only show those risks that match the likelihood you clicked.

5.1.2. Vulnerability Charts

- Vulnerabilities by Category breaks down your identified vulnerabilities by category and severity within each category. Clicking a bar in the chart will filter the table below to show just those vulnerabilities with the category and severity you clicked.

5.1.3. Host Charts

- Active Hosts by OS list the different Operating Systems across the x-axis of the chart along with the number of Hosts using them displayed above each of the bars. Clicking a bar in the chart will drill down to display specific operating systems in that general OS category and filter the table below to show just those hosts.

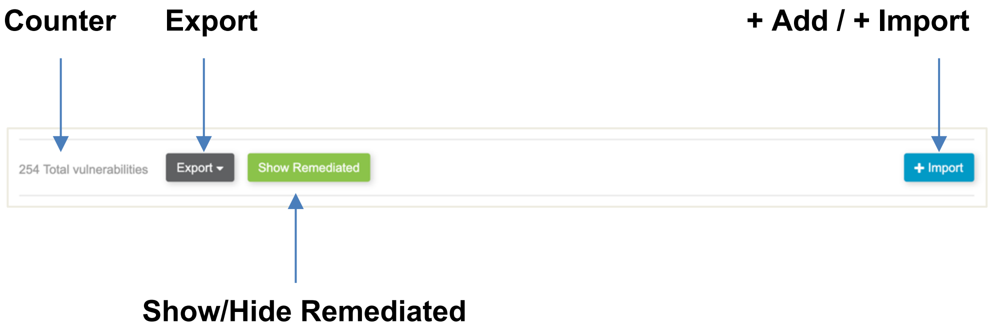
5.2. Export/Import Bar

Displayed just beneath the Interactive Charts, the Export/Import bar includes a counter for the entries in the Data Table and an Export Button for exporting the data.

The Risks page includes the an +Add Risk button for Admins to create new risks.

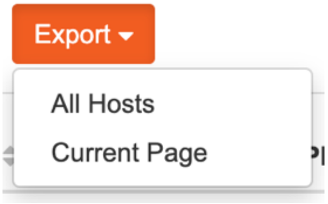
The Vulnerabilities page includes two additional buttons:

- A green Show/Hide Remediated toggle button will display for all users when there are vulnerabilities that have been automatically remediated by the system. When remediated vulnerabilities are displayed, they will be tagged with a green Remediated icon.
- An Import button will display for Admins and allow them to import a new dataset.



5.2.1. Data Table Exporting

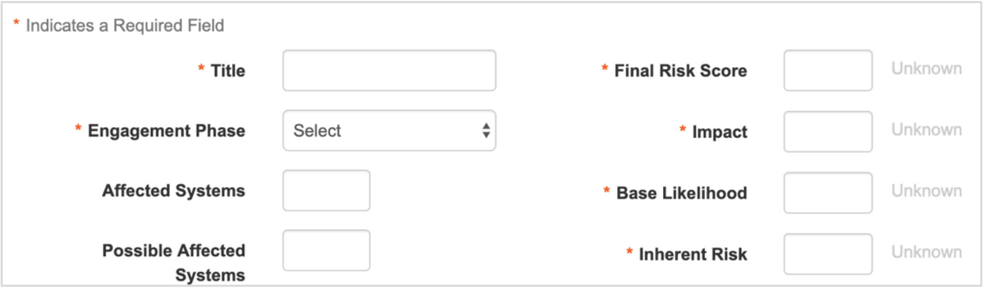
All Users can export the Data table to a CSV file. Simply click **Export** to select whether to export the **Current Page** (using the filters and sorting that selected), or **All Risks/Vulnerabilities/Hosts**. Depending on your browser and its settings, you may be prompted to select a location to which the CSV will be saved.



5.2.2. Adding Risks

Only Admins can add a new Risk by clicking + Add Risk

When adding a Risk, the required fields are indicated by a red asterisk * next to the field label. Admins are encouraged to enter information into the other fields for the new Risk when it is created.



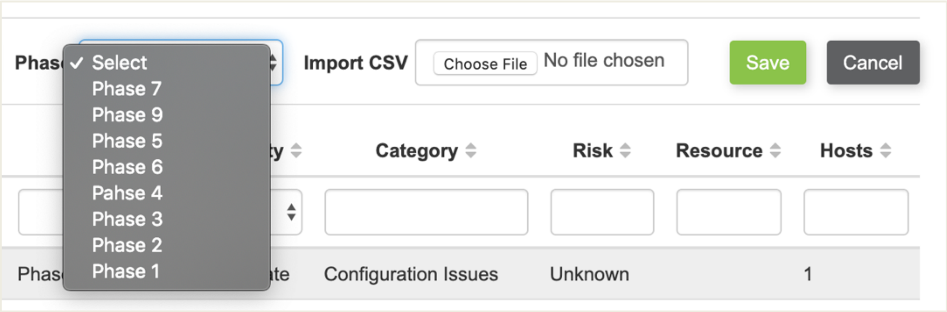
* Indicates a Required Field

* Title		* Final Risk Score		Unknown
* Engagement Phase	Select	* Impact		Unknown
Affected Systems		* Base Likelihood		Unknown
Possible Affected Systems		* Inherent Risk		Unknown

5.2.3. Importing Vulnerabilities

Only Admins can import Vulnerabilities. The Vulnerabilities must be in a standard CSV format, such as one generated by a Nessus scan. To import a Vulnerabilities CSV:

1. Click + Import.
2. Use the Phase drop down list to select the appropriate Phase for the imported vulnerabilities.
3. Click Choose File to browse to the CSV file to be imported.
4. Click Save.



ty	Category	Risk	Resource	Hosts
Phas te	Configuration Issues	Unknown		1

5.3. Hosts, Risks, and Vulnerability Details

Click the blue Risk Title, Vulnerability, or Host Name in the data table to view detailed information and adjust Remediation status information.

- Risk Details includes fields to edit the Risk.
- Vulnerability Details shows information about the Title, Engagement Phase, Scan Details, Category, Service, Port number, a description and the Remedy. A data table of Hosts with that Vulnerability are displayed beneath the details. If the Vulnerability has been remediated on one or more hosts, a Show Remediated button will display to view those hosts. .
- Host Details includes the IP Address, OS, OS Confidence, and Status. Status indicates whether the Host is active, offline, or retired. A data table displays a list of Vulnerabilities for that host and the severity. If the host had vulnerabilities that are no longer present on that host, a Show Remediated button will display to view the remediated vulnerabilities.

5.3.1. Information & Assignments Sidebar

Located on the right-hand side of the Detail view for Risks, Hosts, and Vulnerabilities is a sidebar section that lists additional details and tracking fields. Admins and Managers can assign Remediation Status, Remediation Resource, Target Remediation Date, and Remediated Date on a Risk or Vulnerability.

5.3.2. Host Status – Offline & Retired

When a host is not found on a new import file, the system will mark that host as “Offline”. The assumption is that this host is still active and just off the network when the scan was performed. However, there is a scenario where the host could have been retired.

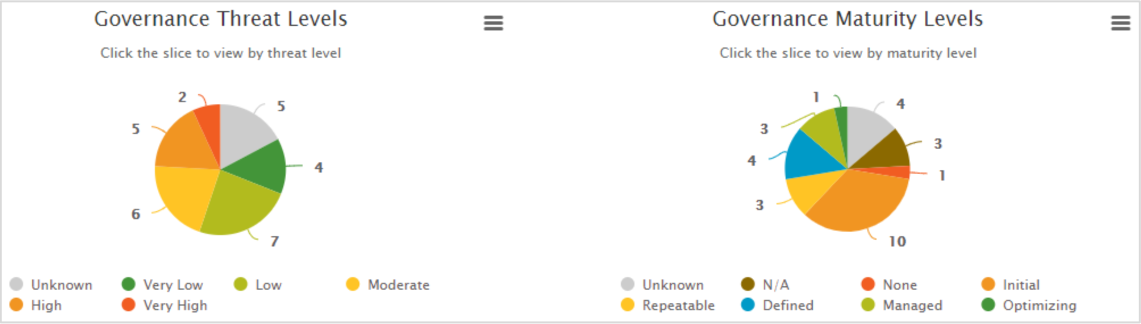
- On the Hosts search page, a checkbox will display for Hosts that are in “Offline” or “Retired” status.
- When one or more hosts are selected, a menu option to Update Status will be available with the ability to update all selected hosts as either “Offline” or “Retired”.
- On the Host detail page, the Status field will be an editable drop-down when the host’s current status is “Offline” or “Retired” and allow users to update the status to either “Retired” or back to “Offline”.

When a Host’s status is changed from “Offline” to “Retired”, it will trigger the system to do the comparison logic to see if any vulnerabilities associated to the Host can be remediated. If a Vulnerability no longer has any active or offline Hosts, it will be remediated; the Vulnerability’s Remediated Date will be set to the last import date, the Vulnerability’s Remediation Status will be set to “Fully Mitigated” and the Vulnerability will no longer show up in the active view on the Vulnerability search page.

If a Vulnerability has active and offline hosts, no changes will be made. If a Host’s status was updated to “Retired” by accident and is set back to “Offline”, the system reactive any affected Vulnerabilities and will restore its last Remediated Date and Remediated Status.

6. Governance

Governance controls can be viewed and managed after a Governance assessment has been completed and the results are uploaded to the portal.



6.1. Controls

Governance controls are displayed in two different charts, breaking them down by their Threat Level and their Maturity Level. Clicking on the various threat level or maturity level pie slices will filter the table of controls under the graphs by that threat or maturity level.

6.1.1. Importing Controls

Only Admins can import the results of a Governance Assessment (in CSV format). To import controls:

1. Click **Import+**.
2. Click **Choose File** to browse to the CSV file.
3. Select the file and click **Open**.
4. Click **Save**.

6.1.2. Adding a Control

Only Admins can add controls manually. To add a control:

1. Click **Add Governance**.
2. Enter the required information about the control, including the Name and Category.
3. Select the required Threat Level and Maturity Level using the drop-down lists.
4. Enter a description and any notes about the control (optional), and then click **Save Governance Control.**

6.1.3. Assigning a Remediation Resource to a Control

Admins and Managers can assign controls:

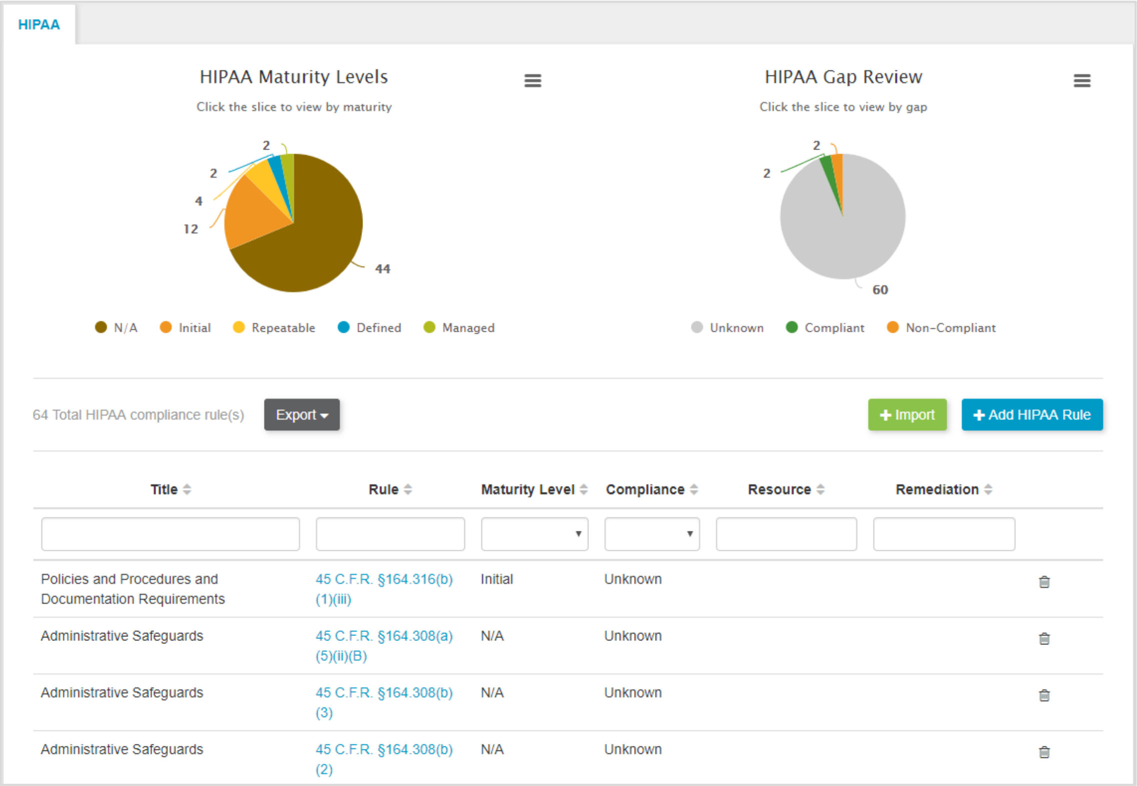
1. In the Governance Control table below the graphs, click on the name of the control for which you wish to add a resource.
2. In the Assignments section, use the drop-down list to select a **Remediation Resource**. This can be a group or an individual, depending on your resource setup.
3. To remove a Resource Assignment, use the drop-down list to select **None** as the Remediation Resource.
4. Click **Save Governance Control** to save the resource assignment.

6.1.4. Removing a Governance Control

To remove a Governance control from the list of controls, click the trashcan icon to the right of the Maturity Level of the control and then click the confirmation icon.

7. Compliance

The NGRM Security Portal supports compliance assessment reporting such as HIPAA. Compliance Rules are displayed in two different charts, breaking them down by their Maturity Level and their Gap Review compliance status. Clicking on the various maturity level or Gap Review pie slices will filter the table of controls under the graphs.



64 Total HIPAA compliance rule(s)

Title	Rule	Maturity Level	Compliance	Resource	Remediation	
Policies and Procedures and Documentation Requirements	45 C.F.R. §164.316(b)(1)(iii)	Initial	Unknown			🗑
Administrative Safeguards	45 C.F.R. §164.308(a)(5)(ii)(B)	N/A	Unknown			🗑
Administrative Safeguards	45 C.F.R. §164.308(b)(3)	N/A	Unknown			🗑
Administrative Safeguards	45 C.F.R. §164.308(b)(2)	N/A	Unknown			🗑

7.1. Importing and Editing Compliance Data

7.1.1. Importing

Only Admins can import the results of a compliance assessment (in CSV format). To import compliance data:

1. Click **Import+**.
2. Click **Choose File** to browse to the CSV file.
3. Select the file and click **Open**.
4. Click **Save**.

7.1.2. Viewing Rules

To view a specific rule, simply click the rule number's link in the rule list.

7.1.3. Editing Compliance Rules

Admins can edit rules they are viewing by updating any of the fields in the rule details.

1. When editing Compliance rules, you must enter or select information in the Rule, Section Title, Compliance and Maturity Level fields.
2. Upon completing any edits, click **Save Rule**.

7.1.4. Assignments

Admins and Managers can manage assignments.

1. In the Compliance Rules table below the graphs, click on the name of the rule for which you wish to add a resource.
2. In the Assignments section, use the drop-down list to select a **Remediation Resource**. This can be a group or an individual, depending on your resource setup.
3. You can also set the **Remediation Status** at this time using the drop-down list.
4. To remove a resource assignment, use the drop-down list to select **None** as the Remediation Resource.
5. Click **Save Rule** to save the resource assignment.

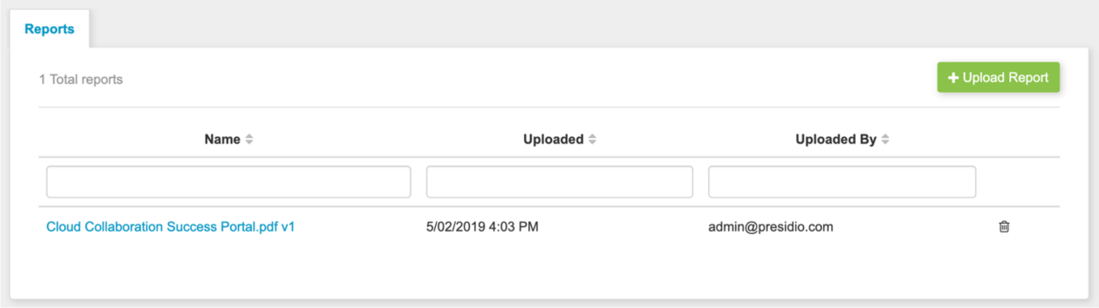
7.1.5. Adding Rules (Admins Only)

1. Click **+Add Rule**.
2. Enter the required information about the rule, including the Rule and Section Title.
3. Select the required Compliance and Maturity Level using the drop-down lists.
4. Enter any optional information about the rule and then click **Save Rule**.

8. Reports

8.1. Uploading Security Reports

All roles have access to view security reports uploaded to the NGRM portal. These will typically be the full security assessment reports generated by Presidio Security Professionals for specific engagements. They can be PDF or Microsoft Office compatible file types. Manager and Customer users can only download and view the reports assigned to their customer name or company. Admins have full authority to add, edit and delete reports.



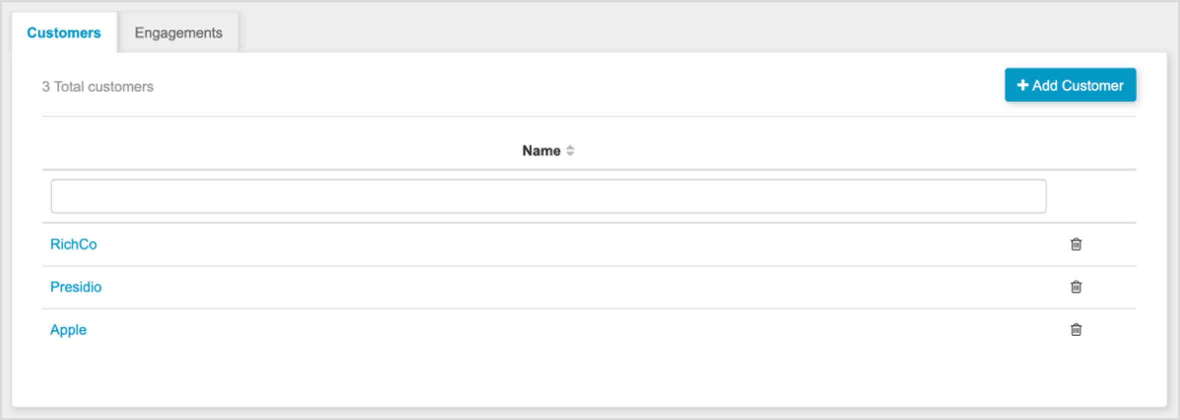
1 Total reports

Name	Uploaded	Uploaded By	
Cloud Collaboration Success Portal.pdf v1	5/02/2019 4:03 PM	admin@presidio.com	🗑

To upload a report, an Admin user would click **+ Upload Report**, click **Choose File**, and browse to the report they wish to upload. Once a report has been selected, they would then click **Save** to upload the file to the portal.

9. Customers (Admins Only)

The Customers page allows admins to add/edit/delete customers and engagements to the NGRM Portal.



3 Total customers

Name ⇕	
RichCo	🗑
Presidio	🗑
Apple	🗑

9.1. Customers Tab

Here, Admins can view the list of active customers in the NGRM portal.

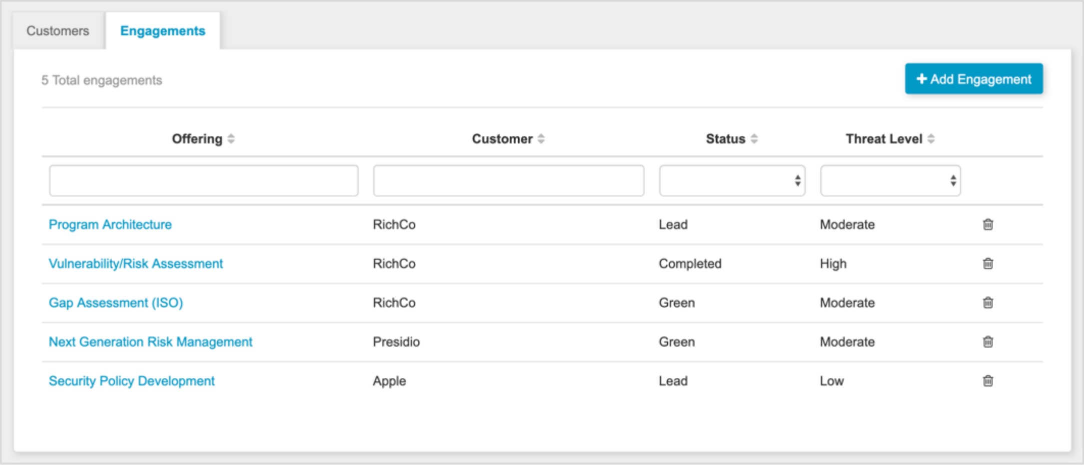
9.1.1. Adding & Deleting Customers

To add a new Customer, click **+Add Customer**, enter their name in the required field and click **Save Customer.**

To delete a Customer, click the trashcan icon next the Customer name, and confirm the deletion by clicking the confirmation icon.

9.2. Engagements Tab

The Engagements tab allows Admins to create multiple engagements for individual customers to help them track their progress through the various engagements they may have with the NGRM team.



5 Total engagements

Offering ⇕	Customer ⇕	Status ⇕	Threat Level ⇕	
Program Architecture	RichCo	Lead	Moderate	🗑
Vulnerability/Risk Assessment	RichCo	Completed	High	🗑
Gap Assessment (ISO)	RichCo	Green	Moderate	🗑
Next Generation Risk Management	Presidio	Green	Moderate	🗑
Security Policy Development	Apple	Lead	Low	🗑

9.2.1. Adding Engagements

1. Click **+Add Engagement**.
2. Use the selection drop down lists to enter the required information for the engagement.
3. If known, enter the risk score in the optional field.
4. Click **Save Engagement**.

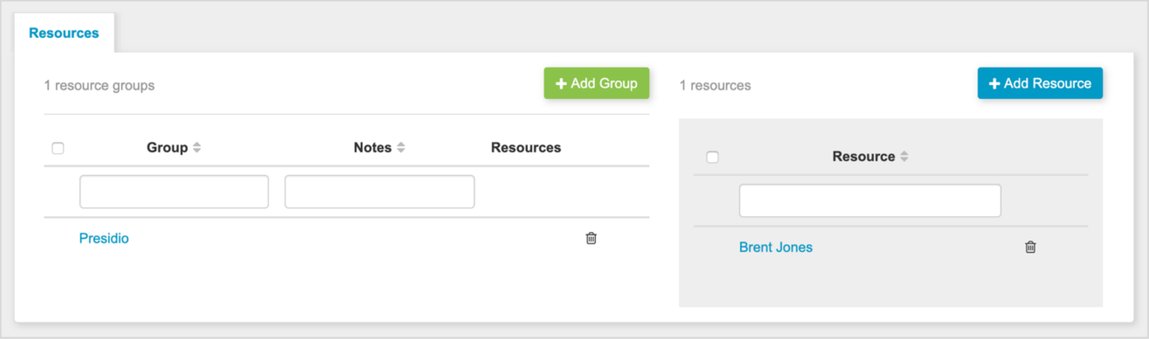
9.2.2. Adding/Deleting Phases

You can only add phases once there is at least one engagement for a customer.

1. Click the name of an engagement to view the engagement details.
2. Click **+Add Phase**.
3. Enter the name of the phase (required) and an optional risk score.
4. Click **Save Phase**.
5. To delete a phase, click the trashcan icon next the phase score of the phase you wish to delete, and then click the confirmation icon.

10. Resources

Resources are the Individuals, Teams or Groups to whom Risk, or Vulnerabilities can be assigned for remediation. You must add resources to the system before you can assign them to a group.



1 resource groups

□	Group	Notes	Resources	
	Presidio			🗑

1 resources

□	Resource	
	Brent Jones	🗑

10.1.1. Adding & Editing Resources

Click **+ Add Resource** to create a new resource. You are required to enter a name for the Resource before you can save it. Once you've named the resource and added any optional notes, click **Save Resource.**

Click the name of the resource to edit the name or notes for that resource. If the resource is assigned to a Group, you can also delete that association by clicking the delete icon in the Group association table for that resource.

10.1.2. Adding Groups

There are two ways to add a resource group:

- You can add a group by clicking **+ Add Group**, entering a group name and any notes, and clicking **Save Group**.
- You can add a group by selecting the check box next to one or more resources and clicking **Create a New Group**, at which point you will be prompted to enter a group name and any notes. To save this group, click **Save Group**.

10.1.3. Assigning Resources to an Existing Group

You can add one or more resources to an existing group by selecting the check box next to one or more resources and clicking **Assign to Existing Group**, at which point you will be prompted to select a group from a drop-down list. After selecting a group, click **Assign**.

10.1.4. Deleting Groups or Resources

To delete a Group or a Resource, simply click the delete icon next to the group or Resource you wish to delete. Confirm your decision by clicking the check mark icon or cancel it by clicking the cancel icon.

Document Revision History

Revision	Date	Notes
0.5	05/31/2018	First Draft
1.0	06/14/2018	Final version for NGRM Portal 2.0
2.1	05/03/2019	Added updates for version 2.1