



# Vendor Risk Management User Guide



## Table of Contents

Overview.....	2
<b>1 Vendor Risk Management.....</b>	<b>3</b>
1.1 Assessment Campaigns .....	6
1.1.1 Step 1: Select or Create Assessment Template. ....	6
1.1.2 Step 2: Schedule Details.....	9
1.1.3 Step 3: Verify and Launch. ....	11
1.2 Risk Report .....	15
1.3 Risk Remediation.....	18
1.3.1 Step 1: Select Assessment.....	18
1.3.2 Step 2: Setup Remediation .....	20
1.3.3 Step 3: Verify and Save .....	21
1.4 Risk Register .....	25
1.5 Maturity Progress.....	29

## Overview

This User Guide outlines the steps to conduct a campaign and produce reports. The steps go through the process of creating an asset within the business hierarchy and associating questions to conduct a campaign which results in an assessment report. The experience of completing the steps in this User Guide will enable the administrator to tailor complex campaigns for each organization.

### What we do!

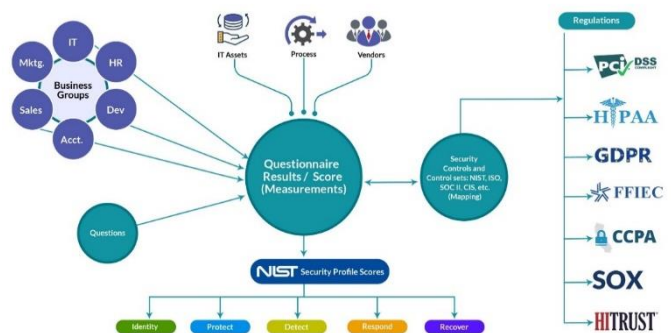
Securends GRC is an accessible SaaS solution that helps achieve a reliable enterprise security score through a simple interface. It can be managed quarterly or annually, even by those who lack experience with managing security or compliance controls. The Securends GRC method of completing risk assessments includes flexible scoring and configuration of the questions, answers, and measurements with a choice of templates for quick implementation.

Assessments are applied to operational activities and security control requirements. Each assessment adds to the enterprise posture score for security and privacy. The current profile is automatically updated and compared with the master target profile to show maturity progress. Participants interact with the questionnaire for measure responses or utilize the capability to re-assign when delegation or additional expertise is required. The participant(s) can add evidence and comments for review before it is presented to audit.

### Why Securends GRC?

Achieve a reliable Enterprise Security Posture that is resilient in a dynamic infrastructure and regulated environment

The Securends GRC application develops an overall enterprise score which is comprised of a questionnaire based on risk management, remediation of compliance and audit requirements. The questionnaires are associated with assets, control sets and business units, supplying a multi-view measurement perspective. Encompassing all areas of an organization, external vendors, or external assessments; the aggregation leads to an enterprise security posture score that goes beyond a two-dimensional spreadsheet.



Product Version	Document Revision	Date
Securends GRC Vendor Risk Management User Guide 1.0	1.0	

# 1 Vendor Risk Management



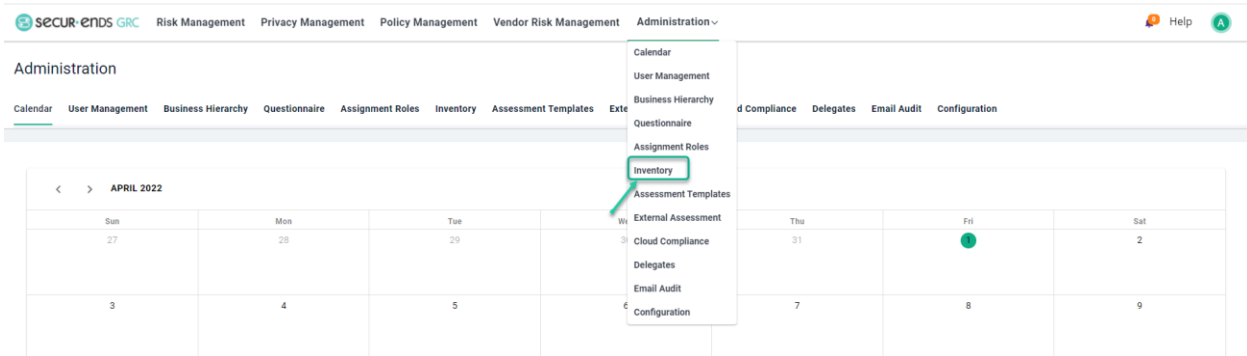
An easy user interface to drive adoption in the assessment process for third party vendors. Standardized formats to increase success in managing vendors, partners, service providers, and more.

- Dashboard
- Assessment Campaigns
- Assessment Reports
- Risk Report
- Risk Remediation
- Risk Register
- Maturity Progress

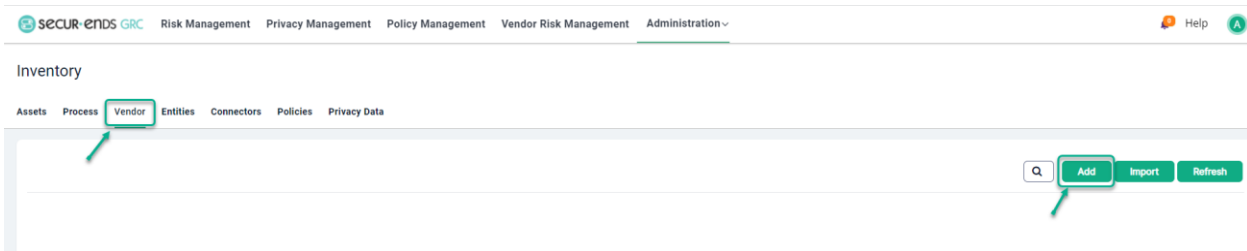
Note: For Vendor Risk Management select Vendor in Inventory.

Add a Vendor under the Inventory.

Select the **Inventory** option in **Administration** drop-down list.



Select **Vendor** and click the **Add** button.



Name the Vendor and then assign a **Vendor Owner** (by selecting the user in the contacts or add new user as appropriate).

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Add Vendor

Setup Vendor

Name\*

Vendor Owner\*  Add

Vendor Type

Vendor EIN

Vendor DUNS Number

Vendor Code

Vendor Address

Assign Business Unit/Department/Division  No  Yes

Questionnaire Source  Control Set

Enter **Vendor Type, Vendor EIN, Vendor DUNS Number, Vendor Code and Vendor Address.**

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Add Vendor

Setup Vendor

Name\*

Vendor Owner\*  Add

Vendor Type

Vendor EIN

Vendor DUNS Number

Vendor Code

Vendor Address

Assign Business Unit/Department/Division  No  Yes

Questionnaire Source  Control Set

Assign it to a level within the Business Hierarchy.

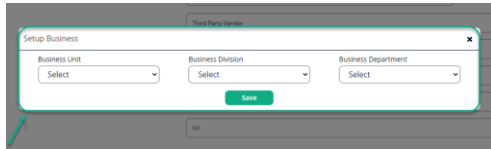
Vendor Address

Assign Business Unit/Department/Division  No  Yes

Questionnaire Source  Control Set

Save

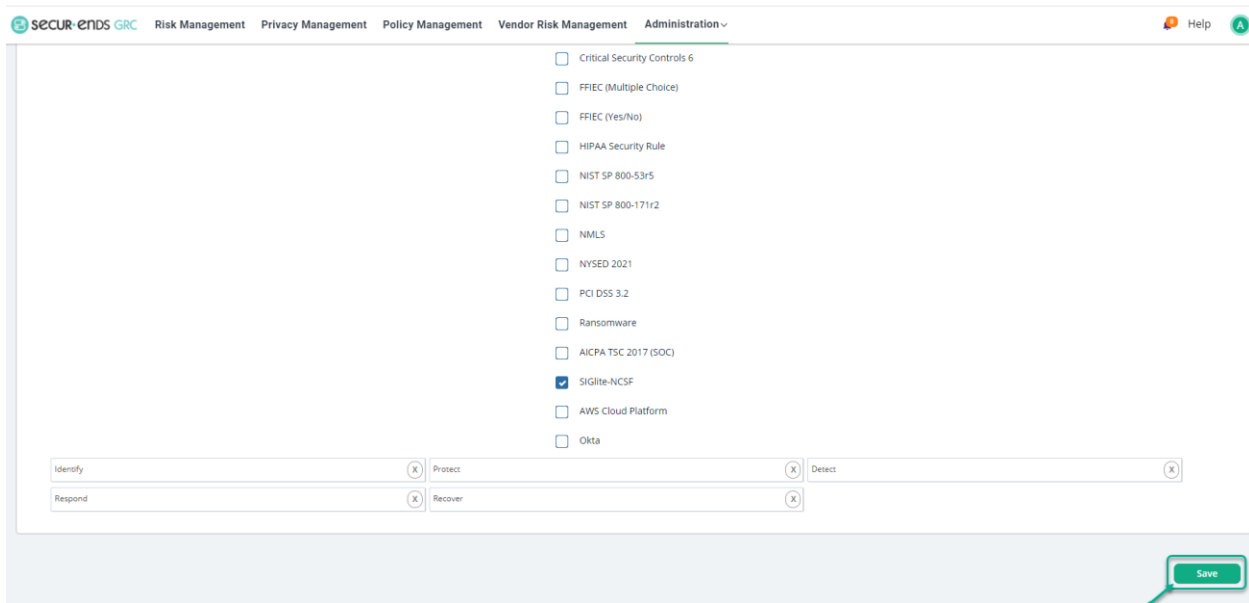
Select the **Yes** radio button and assign it to a business level and click the **Save** button.



Click the **Control Set** radio button from **Questionnaire Source**.

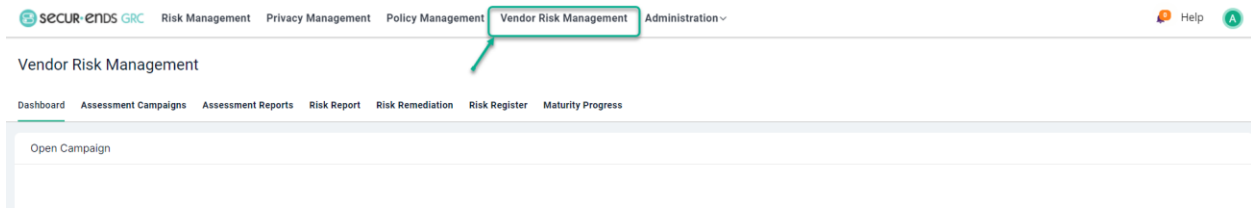
Select box for **SIGlite-NCSF**.

Click the **Save** button in the bottom right corner of the page.

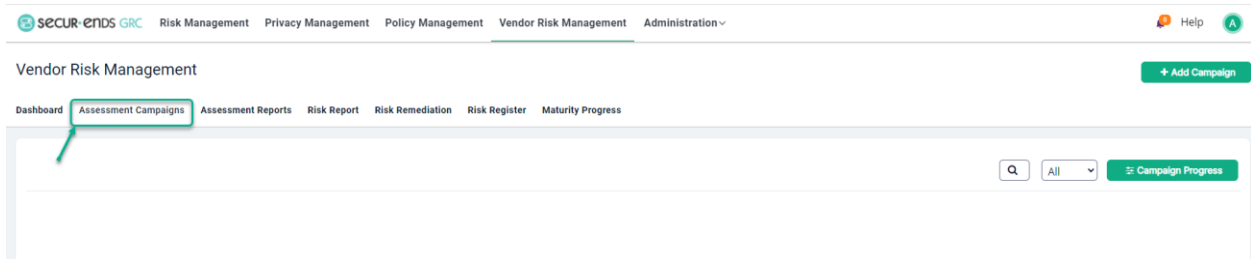


## 1.1 Assessment Campaigns

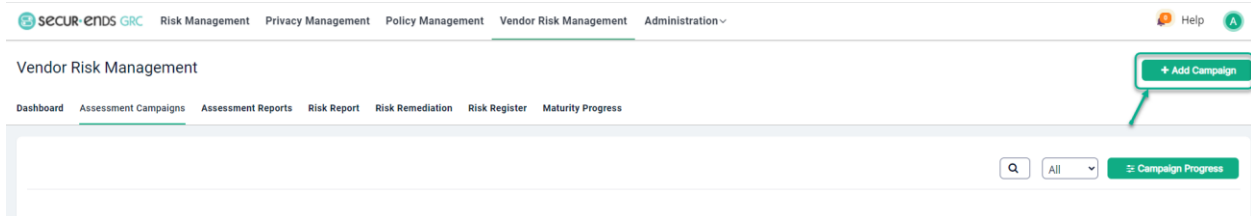
Select the **Vendor Risk Management** tab on the main menu.



Select **Assessment Campaigns** Tab.



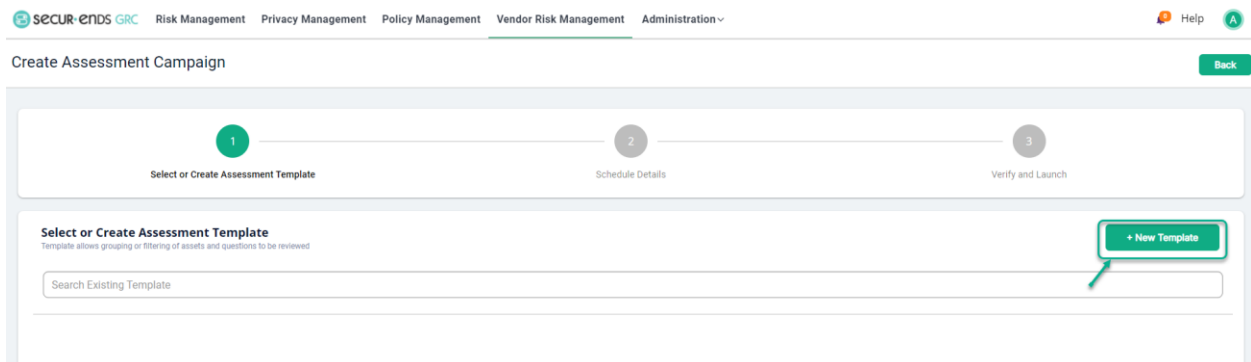
Click the **Add Campaign** button to follow three step process.



The three-step process page is launched.

### 1.1.1 Step 1: Select or Create Assessment Template.

Click the **New Template** button to create new Assessment Template.



## Enter a **Template Name** and **Description**.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

Create Assessment Campaign Back

1 Select or Create Assessment Template 2 Schedule Details 3 Verify and Launch

Template Name\* Template Name

Description\* Description

Inventory Type\*  Vendors

Close Save

## Click the **Vendors** radio button and select the Vendor from the dropdown list.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

Create Assessment Campaign Back

1 Select or Create Assessment Template 2 Schedule Details 3 Verify and Launch

Template Name\* Third Party Vendor Assessment

Description\* Third Party Vendor Assessment

Inventory Type\*  Vendors

Vendor Third Party Vendor Assessment \*

Search

Select all

Third Party Vendor Assessment

Vendor

Third Party Vendor Assessment

Yes No

View Questionnaire

Close Save

## Click the **Yes** radio button to select all questions.

Or, click the **No** radio button and then click the **Select/Unselect Questionnaire** button.

Vendor

Include All Questions

Actions

Third Party Vendor Assessment

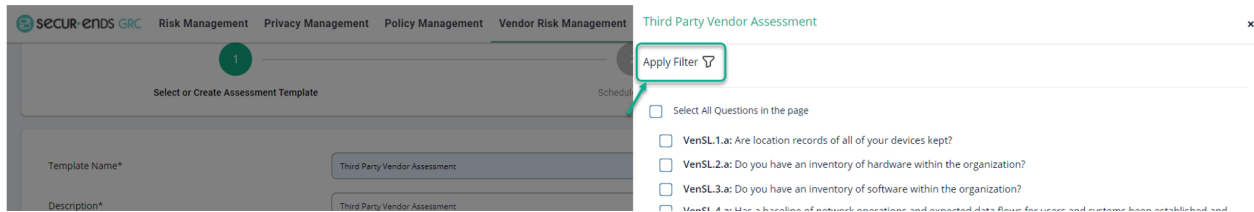
Yes No

Select/Unselect Questionnaire

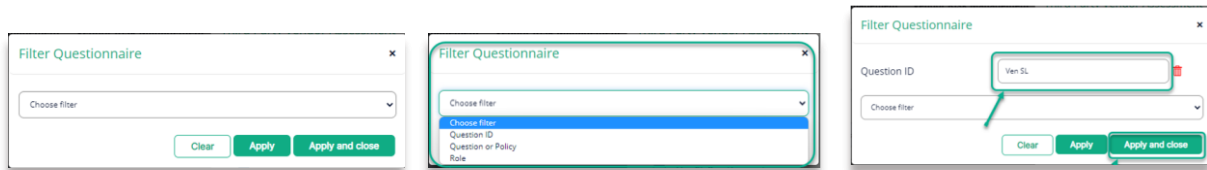
Close Save



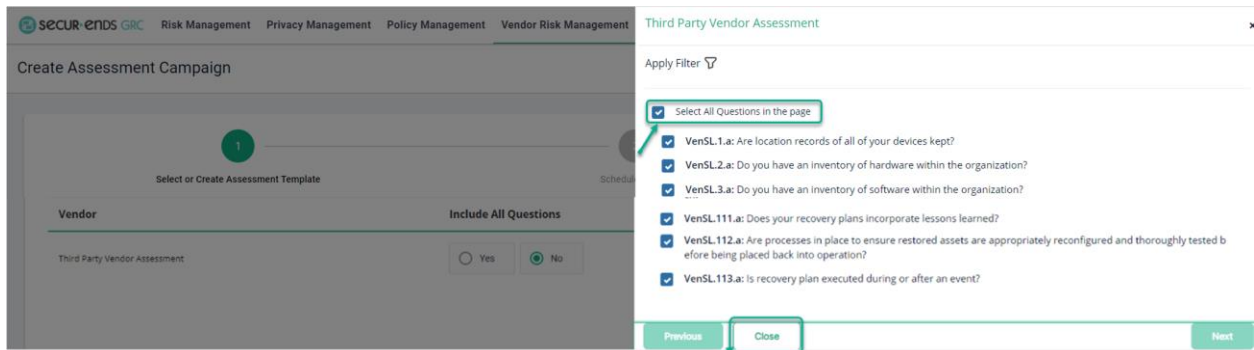
Click the **Apply Filter** symbol.



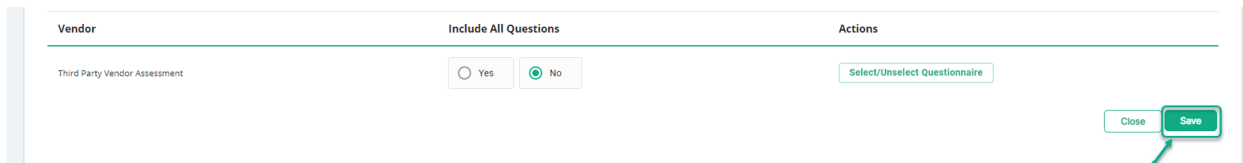
At the pop-up window, choose Filter **Question ID/ Question or Policy / Role**. Enter Question ID and then click on **Apply and Close** button.



Check the box for **Select All Questions** in the page and click the **Close** button.



Click the **Save** button.



Select the Assessment Template that was created.

The screenshot shows the 'Create Assessment Campaign' page in the SecurEnds GRC system. The page title is 'Create Assessment Campaign' with a 'Back' button in the top right. A progress bar at the top indicates three steps: 1. Select or Create Assessment Template (active), 2. Schedule Details, and 3. Verify and Launch. Below the progress bar, the 'Select or Create Assessment Template' section is visible. It includes a search bar for existing templates, a '+ New Template' button, and a list of templates. The first template, 'Third Party Vendor Assessment', is highlighted with a green box and a 'Select Template' button next to it.

### 1.1.2 Step 2: Schedule Details

## Assessment Configuration

Enter Assessment Campaign Name.

The screenshot shows the 'Create Assessment Campaign' page in the SecurEnds GRC system, now at Step 2: Schedule Details. The progress bar shows Step 2 is active. The 'Assessment Configuration' section is visible, showing the 'Third Party Vendor Assessment' template. The 'Assessment Campaign Name' field is highlighted with a green box and contains the text 'Campaign Name'. Below this, there is a checkbox for 'Create a Target Campaign' which is currently unchecked. The 'Start Date' and 'End Date' fields are both set to '04/03/2022'. At the bottom, the 'Assessment Campaign Reviewer' section has three radio buttons: 'Asset Owner' (selected), 'Role Owner', and 'Alternate Reviewer'.

Note: For creating Target Campaign select “Create a Target Campaign” option and enter Alternate Reviewer.

This is a close-up screenshot of the 'Create Assessment Campaign' page, Step 2: Schedule Details. It focuses on the 'Assessment Campaign Name' field, which contains 'Third Party Vendor Target Questionnaire'. The 'Create a Target Campaign' checkbox is checked and highlighted with a green box. The 'Start Date' and 'End Date' fields are both set to '04/03/2022'.

Select a "Start Date" and "End Date".

The screenshot shows the 'Assessment Configuration' page for a 'Third Party Vendor Assessment'. The 'Assessment Campaign Name' is 'Third Party Vendor Questionnaire'. The 'Start Date' is '04/03/2022' and the 'End Date' is '04/03/2022'. A calendar for April 2022 is visible, with the 3rd and 4th highlighted. The 'Assessment Campaign Reviewer' is set to 'Asset Owner'.

Select **Asset Owner/Role owner/Alternate Reviewer**.

The screenshot shows the 'Assessment Configuration' page with the 'Assessment Campaign Reviewer' options highlighted: 'Asset Owner' (selected), 'Role Owner', and 'Alternate Reviewer'. The 'Start Date' is '04/03/2022' and the 'End Date' is '04/30/2022'. The 'Final Approver' checkbox is unchecked. The 'Campaign Reminders' section has 'Send reminder email to reviewer' unchecked. The 'Campaign Instructions' dropdown is set to 'Default'. 'Back' and 'Next' buttons are at the bottom right.

Select **Final Approver** option and enter the user details (Final Approver can review the answers given by the Reviewer).

The screenshot shows the 'Final Approver' section with the 'Final Approver' checkbox checked. A search field is present with a 'Clear' button. The 'Campaign Reminders' section has 'Send reminder email to reviewer' unchecked.

Select **Campaign Reminders** option (By selecting this option, the reminder email can send to Reviewer). The **Campaign Instructions** dropdown menu provides the option for the administrator to change the default message at the top of the campaign to a note or instructions for the reviewer. Click the **Next** button to advance to the next step.

The screenshot shows a form with the following elements:

- Final Approver
- Campaign Reminders** (highlighted with a green box)
  - Send reminder email to reviewer
- Campaign Instructions** dropdown menu (set to 'Default')
- and  buttons (the 'Next' button is highlighted with a green box)

### 1.1.3 Step 3: Verify and Launch.

Click the **Preview** and then the **Launch** button.

The screenshot shows the 'Launch Campaign' step in the 'Create Assessment Campaign' process. The progress bar indicates three steps: 1. Select or Create Assessment Template, 2. Schedule Details, and 3. Verify and Launch (current step).

**Launch Campaign**

Third Party Vendor Questionnaire Ready

04/03/2022 Campaign Start Date	04/30/2022 Campaign End Date
User@securends.com Reviewer Email ID	N/A Final Approver Email ID

**Questionnaire - preview**

Are location records of all of your devices kept?

0-Not Enabled  1-Initial  2-Repeatabe  3-Defined  4-Managed  5-Optimized

The screenshot shows a dialog box titled 'Launch Campaign' with the following content:

Do you want to launch this campaign?

Send email notification to all reviewers that are part of the campaign  Exclude notification to selected reviewers

Open the Actions menu and select View item.

The screenshot shows the 'Vendor Risk Management' dashboard. At the top, there are navigation tabs: Risk Management, Privacy Management, Policy Management, Vendor Risk Management (selected), and Administration. A search bar and a 'Campaign Progress' button are also visible. Below the navigation, there's a sub-menu with 'Assessment Campaigns' selected. The main content area displays a table with columns: Name, Status, Start Date, End Date, and Actions. The first row is 'Third Party Vendor Questionnaire' with a status of 'Open', start date of 'Apr 03, 2022', and end date of 'Apr 30, 2022'. The 'Actions' column for this row has a dropdown menu open, showing options: View (selected), Details, Edit, Close, Remind, and Delete. A green callout box highlights the 'View' option.

On the Assessment Campaign Preview page, select the Assess button on the right.

The screenshot shows the 'Assessment Campaign Preview - Third Party Vendor Questionnaire' page. It features a table with columns: First Name, Last Name, Email, Total, and Pending. The first row contains 'User', 'GRC', 'User@secureends.com', '26', and '26'. An 'Assess' button is located to the right of the 'Pending' column for the first row, highlighted with a green callout box. The page also includes a search bar and a 'Back' button.

The user is presented with the outline of the assessment.

The screenshot shows the 'Assessment' page. At the top, there are buttons for 'Assign User', 'Submit', and 'Back'. The main content area displays the assessment details for 'Third Party Vendor Questionnaire' (Assessment Campaign) and 'User GRC (User@secureends.com)' (Reviewer). A 'DUE IN 27 DAYS' badge is visible. Below this, there's a note: 'Note: Expand each section to complete answers, provide comments and attach document.' The assessment is divided into five sections: Identify (0/5), Protect (0/5), Detect (0/6), Respond (0/6), and Recover (0/4). A 'Submit' button is at the bottom right.

Expand each section to complete answers, provide comments and attach document.

The screenshot shows the 'Third Party Vendor Questionnaire' assessment interface. At the top, there is a navigation bar with 'SECURE ENDS GRC' and various management categories. The assessment title is 'Third Party Vendor Questionnaire' and the reviewer is 'User GRC'. A 'DUE IN 27 DAYS' badge is visible. A progress bar shows '0 answered questions out of 26'. A note states: 'Note: Expand each section to complete answers, provide comments and attach document.' The question is '1 Are location records of all of your devices kept?' with radio button options: '0-Not Enabled', '1-Initial', '2-Repeatabe', '3-Defined', '4-Managed', and '5-Optimized'. There is a 'Clear Selection' button and a text input field for comments. A 'Reassign' button is highlighted with a red box and a red arrow. A document icon with a '0' is also present.

Select **Reassign** button (by selecting this option can reassign the question to another reviewer).

This screenshot is identical to the one above, but the 'Reassign' button is highlighted with a red box and a red arrow, indicating the action to be taken. The rest of the interface, including the question and options, remains the same.

Answer all questions and click the **Submit** button.

The screenshot shows a questionnaire interface. At the top, there is a navigation bar with 'SECUR-ENDS GRC' and several menu items: Risk Management, Privacy Management, Policy Management, Vendor Risk Management, and Administration. A 'Help' icon is also present. The main content area contains two questions. Question 3 asks: 'Are processes in place to ensure restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation?'. It has five radio button options: 0-Not Enabled, 1-Initial, 2-Repeatable, 3-Defined (which is selected), and 4-Managed. Below the options is a 'Clear Selection' button and a text input field labeled 'Enter your comments...'. A 'Reassign' button and a comment icon are also visible. Question 4 asks: 'Is recovery plan executed during or after an event?'. It has five radio button options: 0-Not Enabled, 1-Initial, 2-Repeatable, 3-Defined, and 4-Managed (which is selected). Similar to question 3, it has a 'Clear Selection' button, a text input field, a 'Reassign' button, and a comment icon. At the bottom right of the form, there is a green 'Submit' button with a red arrow pointing to it.

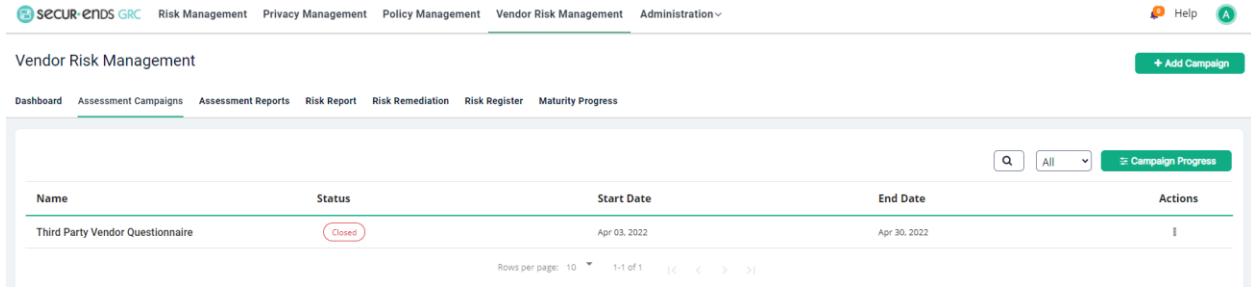
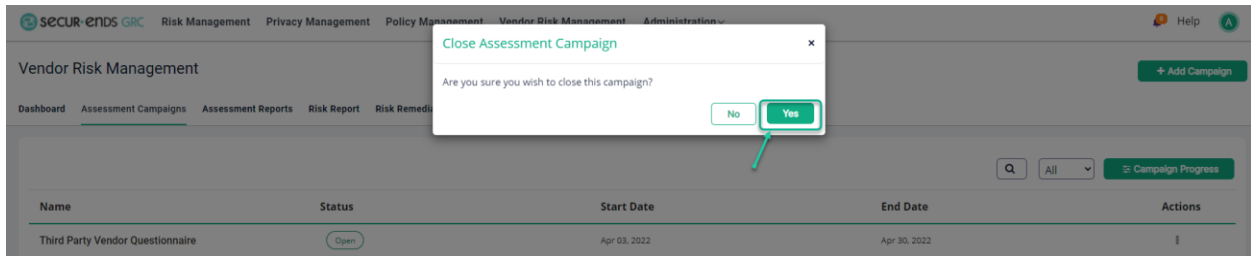
Click the **Back** button.

The screenshot shows an 'Assessment Campaign Preview - Third Party Vendor Questionnaire' page. At the top, there is a navigation bar with 'SECUR-ENDS GRC' and menu items: Risk Management, Privacy Management, Policy Management, Vendor Risk Management, and Administration. A 'Help' icon is also present. Below the navigation bar, there is a search icon and a green 'Back' button with a red arrow pointing to it. The main content area is a table with the following columns: First Name, Last Name, Email, Total, Pending, and an 'Assess' button. The table contains one row with the following data: First Name: User, Last Name: GRC, Email: User@secureends.com, Total: 26, Pending: 0. Below the table, there is a pagination control showing 'Rows per page: 10' and '1-1 of 1'.

Click the Actions menu and select **Close** option to close the campaign.

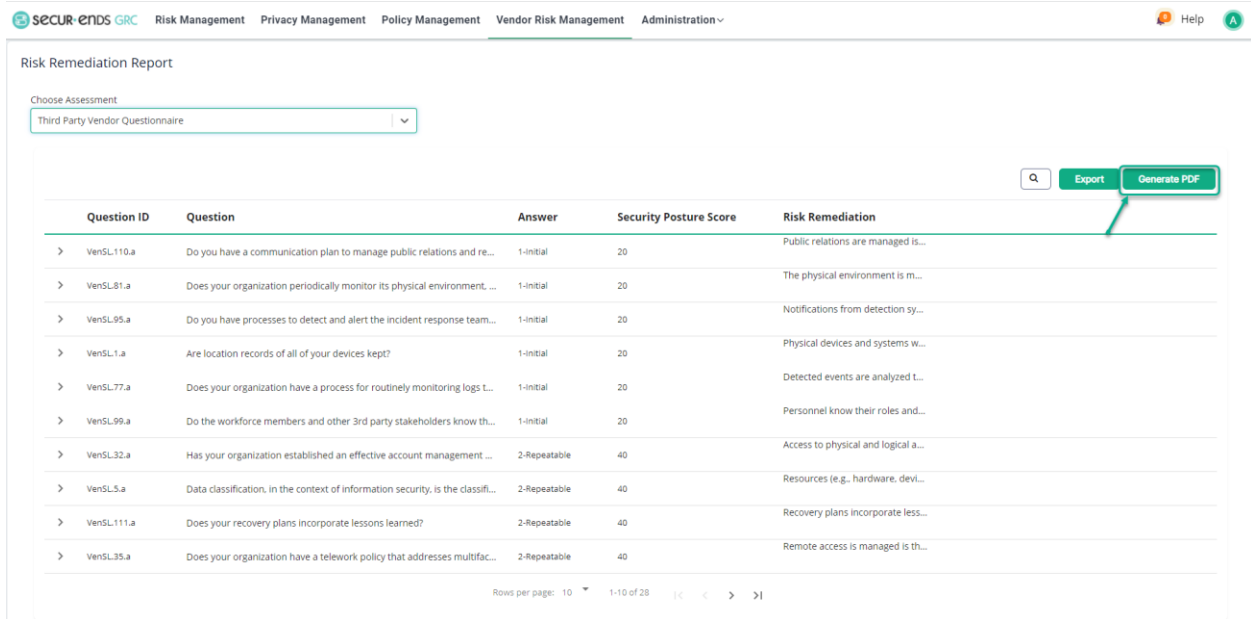
The screenshot shows a 'Vendor Risk Management' dashboard. At the top, there is a navigation bar with 'SECUR-ENDS GRC' and menu items: Risk Management, Privacy Management, Policy Management, Vendor Risk Management, and Administration. A 'Help' icon is also present. Below the navigation bar, there is a '+ Add Campaign' button. The main content area is a dashboard with several tabs: Dashboard, Assessment Campaigns (which is selected), Assessment Reports, Risk Report, Risk Remediation, Risk Register, and Maturity Progress. Below the tabs, there is a search icon, a dropdown menu set to 'All', and a 'Campaign Progress' button. The main content area is a table with the following columns: Name, Status, Start Date, End Date, and Actions. The table contains one row with the following data: Name: Third Party Vendor Questionnaire, Status: Open, Start Date: Apr 03, 2022, End Date: Apr 30, 2022. Below the table, there is a pagination control showing 'Rows per page: 10' and '1-1 of 1'. An actions menu is open for the first row, showing options: View, Details, Edit, Close (which is highlighted with a red box and a red arrow), Remind, and Delete.

Select **Yes** option to close the Campaign.



## 1.2 Risk Report

Click the **Generate PDF** button to generate Risk Remediation PDF Report.





Open or Save the PDF as supplied through the browser interface.

SECUR·ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

### Risk Remediation Report

Choose Assessment  
Third Party Vendor Questionnaire

Export Generate PDF

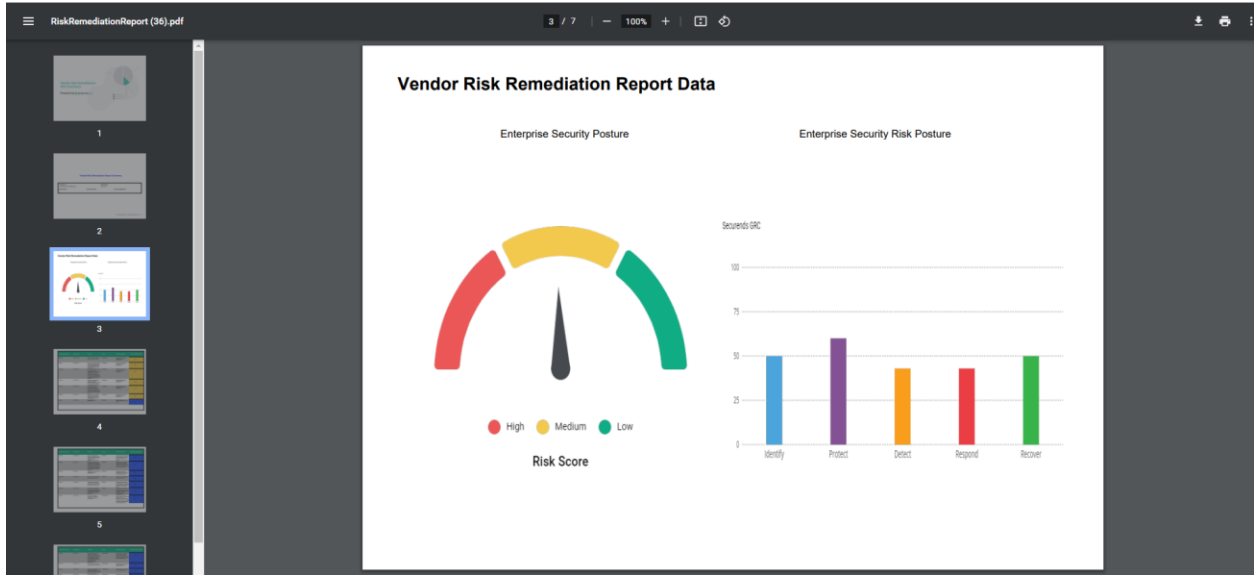
Question ID	Question	Answer	Security Posture Score	Risk Remediation
VenSL110.a	Do you have a communication plan to manage public relations and re...	1-Initial	20	Public relations are managed is...
VenSL81.a	Does your organization periodically monitor its physical environment, ...	1-Initial	20	The physical environment is mo...
VenSL95.a	Do you have processes to detect and alert the incident response team...	1-Initial	20	Notifications from detection sys...
VenSL1.a	Are location records of all of your devices kept?	1-Initial	20	Physical devices and systems w...
VenSL77.a	Does your organization have a process for routinely monitoring logs t...	1-Initial	20	Detected events are analyzed L...
VenSL99.a	Do the workforce members and other 3rd party stakeholders know th...	1-Initial	20	Personnel know their roles and ...
VenSL32.a	Has your organization established an effective account management ...	2-Repeatable	40	Access to physical and logical a...
VenSL5.a	Data classification, in the context of information security, is the classifi...	2-Repeatable	40	Resources (e.g., hardware, devi...
VenSL111.a	Does your recovery plans incorporate lessons learned?	2-Repeatable	40	Recovery plans incorporate less...
VenSL35.a	Does your organization have a telework policy that addresses multifac...	2-Repeatable	40	Remote access is managed is th...

Rows per page: 10 1-10 of 28

RiskRemediationR...pdf Show all

RiskRemediationReport (36).pdf 1 / 7 100%

The image shows a PDF viewer displaying a document titled "Vendor Risk Remediation Plan Summary". The document features a large graphic on the right side consisting of overlapping circles and lines, with a teal-colored segment. The text on the left side of the page reads "Vendor Risk Remediation Plan Summary" in a bold, teal font, followed by "Powered by SECUR·ENDS GRC" in a smaller, teal font. The PDF viewer interface includes a sidebar on the left with thumbnails of the document's pages and a top navigation bar with page number, zoom level, and other controls.



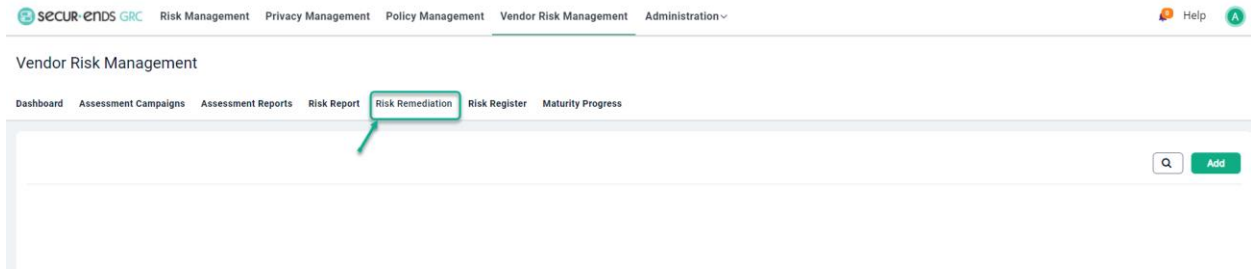
RiskRemediationReport (36).pdf 4 / 7 100%

Presentation Group	Question ID	Question	Status	Risk Remediation	Security Posture Score
Recover	VenSI_113.a	Is recovery plan executed during or after an event?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Detect	VenSI_80.a	Does your organization have a processes and policies for routinely monitoring logs to detect unauthorized and anomalous activities within your network?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Respond	VenSI_98.a	Does your organization have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability of critical systems and security of sensitive data immediately after a crisis situation?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Protect	VenSI_37.a	Does your comprehensive account management process only allow authorized individuals access to the organization's Data and Information Systems?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Protect	VenSI_34.a	Do you have physical protections in place to manage physical security risks, such as a) locks on doors and windows and b) cameras in non-public areas to monitor all entrances and exits?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Identify	VenSI_4.a	Has a baseline of network operations and expected data flows for users and systems been established and managed?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Detect	VenSI_79.a	Is impact of events determined?	3-Defined	Impact of events is determined is the expected result.	65

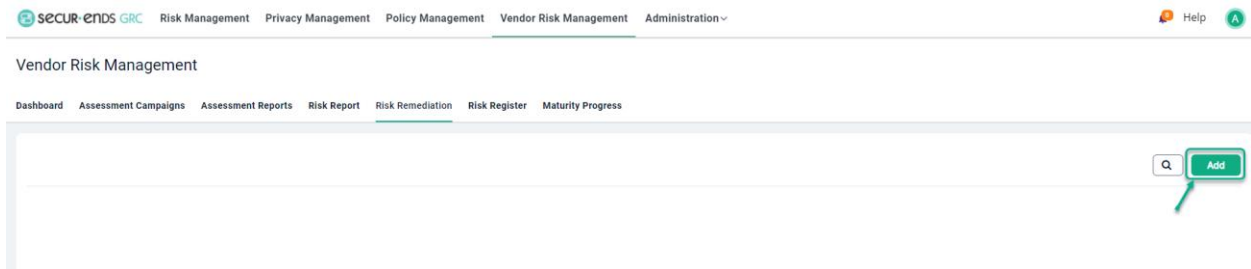
### 1.3 Risk Remediation

#### Creation of Remediation Plan.

Click the Vendor Risk Management tab on the main menu and select Risk Remediation tab.

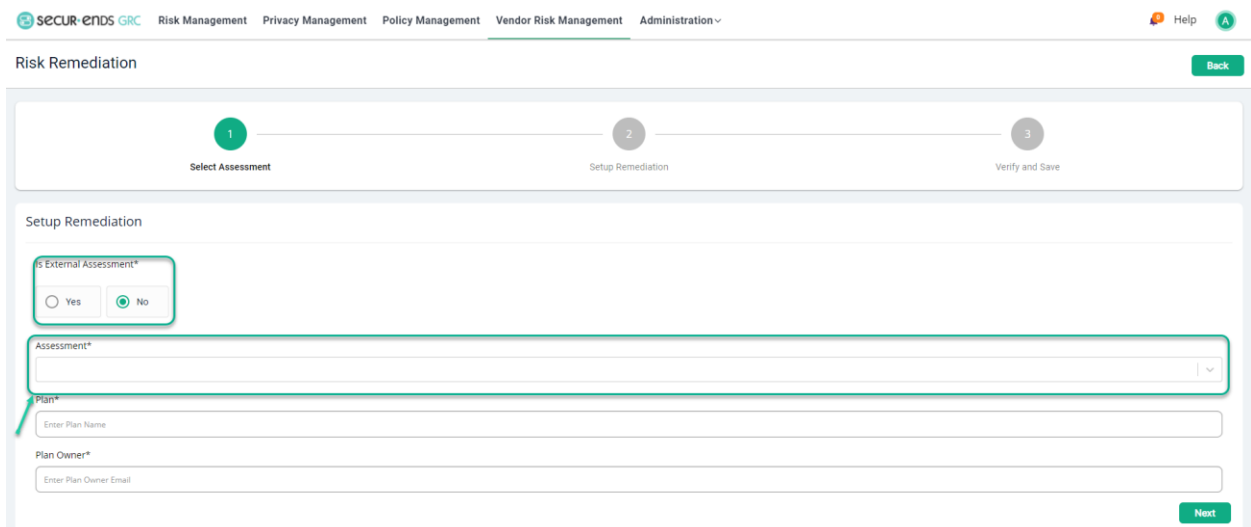


Click the Add button to follow three step process.



#### 1.3.1 Step 1: Select Assessment

Select **External Assessment** option and **Assessment** from the drop-down list.



## Enter a Plan name and Plan Owner.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

Risk Remediation [Back](#)

1 Select Assessment 2 Setup Remediation 3 Verify and Save

Setup Remediation

Is External Assessment\*  
 Yes  No

Assessment\*  
Third Party Vendor Questionnaire

Plan\*  
Enter Plan Name

Plan Owner\*  
Enter Plan Owner Email

[Next](#)

## Click the Next button.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

Risk Remediation [Back](#)

1 Select Assessment 2 Setup Remediation 3 Verify and Save

Setup Remediation

Is External Assessment\*  
 Yes  No

Assessment\*  
Third Party Vendor Questionnaire

Plan\*  
Third Party Vendor Remediation Plan

Plan Owner\*  
User@securends.com

[Next](#)

## 1.3.2 Step 2: Setup Remediation

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration ▾ Help ⓘ

Risk Remediation Back

1 Select Assessment 2 Setup Remediation 3 Verify and Save

Selected Assessment: **Third Party Vendor Questionnaire** Plan Name: **Third Party Vendor Remediation Plan** Plan Owner Email: **User@securends.com**

Remediation Q Next

ID	Presentation Gr...	Questions	Answer	Score	Priority *	Ticket *	Remediation Owner *	Comments	Risk Remediation
> VenSL32.a	Protect	Has your organization established an ...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Access to physical and log
> VenSL110.a	Recover	Do you have a communication plan to ...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Public relations are mana
> VenSL77.a	Detect	Does your organization have a process...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Detected events are analy

Select **Priority** and **Ticket** from the drop-down menu, enter **Remediation Owner** and **Comments** to the rows that have an action listed in the Risk Remediation column.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration ▾ Help ⓘ

Selected Assessment: **Third Party Vendor Questionnaire** Plan Name: **Third Party Vendor Remediation Plan** Plan Owner Email: **User@securends.com**

Remediation Q Next

ID	Presentation Gr...	Questions	Answer	Score	Priority *	Ticket *	Remediation Owner *	Comments	Risk Remediation
> VenSL32.a	Protect	Has your organization established an ...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Access to physical and log
> VenSL110.a	Recover	Do you have a communication plan to ...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Public relations are mana
> VenSL77.a	Detect	Does your organization have a process...	1-Initial	20	Select ▾	Select ▾	Remediation owner		Detected events are analy

Click the **Next** button.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration ▾ Help ⓘ

Selected Assessment: **Third Party Vendor Questionnaire** Plan Name: **Third Party Vendor Remediation Plan** Plan Owner Email: **User@securends.com**

Remediation Q Next

ID	Presentation Gr...	Questions	Answer	Score	Priority *	Ticket *	Remediation Owner *	Comments	Risk Remediation
> VenSL32.a	Protect	Has your organization established an ...	1-Initial	20	2 ▾	Y ▾	User@securends.com		Access to physical and log
> VenSL110.a	Recover	Do you have a communication plan to ...	1-Initial	20	3 ▾	Y ▾	User@securends.com		Public relations are mana
> VenSL77.a	Detect	Does your organization have a process...	1-Initial	20	1 ▾	N ▾	User@securends.com		Detected events are analy

### 1.3.3 Step 3: Verify and Save

Click the **Save** button.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Selected Assessment: **Third Party Vendor Questionnaire** Plan Name: **Third Party Vendor Remediation Plan** Plan Owner Email: **User@securends.com**

Remediation Q Save

Question ID	Presentation Gr...	Questions	Answer	Score	Priority	Ticket	Remediation Owner	Comments	Risk Remediation
> VenSL32.a	Protect	Has your organization established an ...	1-Initial	20	2	Y	User@securends.com		Access to physical and logical assi
> VenSL110.a	Recover	Do you have a communication plan to ...	1-Initial	20	3	Y	User@securends.com		Public relations are managed is th
> VenSL77.a	Detect	Does your organization have a process...	1-Initial	20	1	N	User@securends.com		Detected events are analyzed to l
> VenSL95.a	Detect	Do you have processes to detect and a...	1-Initial	20	4	N	User@securends.com		Notifications from detection syste
> VenSL33.a	Protect	Does your organization require an aut...	2-Repeatable	40	2	Y	User@securends.com		Identities and credentials are issu
> VenSL2.a	Identify	Do you have an inventory of hardware...	2-Repeatable	40	2	N	User@securends.com		Physical devices and systems with
> VenSL111.a	Recover	Does your recovery plans incorporate L...	2-Repeatable	40	3	Y	User@securends.com		Recovery plans incorporate lessor
> VenSL112.a	Recover	Are processes in place to ensure resto...	3-Defined	60	4	N	User@securends.com		Recovery processes and procedu
> VenSL3.a	Identify	Do you have an inventory of software ...	3-Defined	60	1	Y	User@securends.com		Software platforms and applicatic
> VenSL97.a	Respond	Do you collect and analyze post-incide...	3-Defined	60	4	N	User@securends.com		Forensics are performed is the ex

### Click the **Actions Menu** and select **View Report** option.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

Remediation Plan Plan Owner Assessment Type Actions

Third Party Vendor Remediation Plan User@securends.com Internal

Rows per page: 10 1-1 of 1 [C < > >]

View Report Delete

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Remediation Plan Generate PDF Back

Remediation Details

Plan Name : Third Party Vendor Remediation Plan  
 Plan Owner : User@securends.com  
 Assessment : Third Party Vendor Questionnaire

Q

Question ID	Presentation Group	Question	Answer	Security Posture Score	Priority	Ticket	Remediation Owner	Risk Remediation
> VenSL77.a	Detect	Does your organization have a process for rout...	1-Initial	20	1	N	User@securends.com	Detected events are analyzed to l
> VenSL3.a	Identify	Do you have an inventory of software within th...	3-Defined	60	1	Y	User@securends.com	Software platforms and applicatic
> VenSL32.a	Protect	Has your organization established an effective ...	1-Initial	20	2	Y	User@securends.com	Access to physical and logical assi
> VenSL33.a	Protect	Does your organization require an authorized ...	2-Repeatable	40	2	Y	User@securends.com	Identities and credentials are issu
> VenSL2.a	Identify	Do you have an inventory of hardware within L...	2-Repeatable	40	2	N	User@securends.com	Physical devices and systems with

## Generate Remediation Plan Report

Click the **Generate PDF** button.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

Remediation Plan Generate PDF Back

Remediation Details

Plan Name : Third Party Vendor Remediation Plan  
 Plan Owner : User@securends.com  
 Assessment : Third Party Vendor Questionnaire

Question ID	Presentation Group	Question	Answer	Security Posture Score	Priority	Ticket	Remediation Owner	Risk Remediation
> VenSL77.a	Detect	Does your organization have a process for rout...	1-Initial	20	1	N	User@securends.com	Detected events are analyzed to l
> VenSL3.a	Identify	Do you have an inventory of software within th...	3-Defined	60	1	Y	User@securends.com	Software platforms and applicatic
> VenSL32.a	Protect	Has your organization established an effective ...	1-Initial	20	2	Y	User@securends.com	Access to physical and logical assi
> VenSL33.a	Protect	Does your organization require an authorized ...	2-Repeatable	40	2	Y	User@securends.com	Identities and credentials are issu
> VenSL2.a	Identify	Do you have an inventory of hardware within t...	2-Repeatable	40	2	N	User@securends.com	Physical devices and systems wif

Open or Save the PDF.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration Help

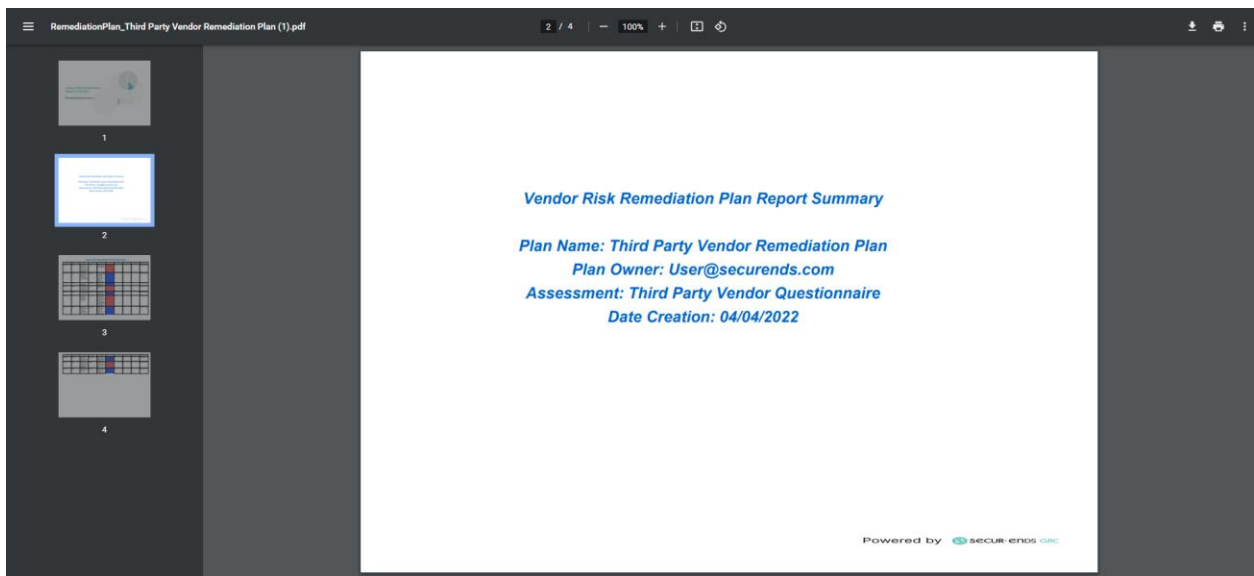
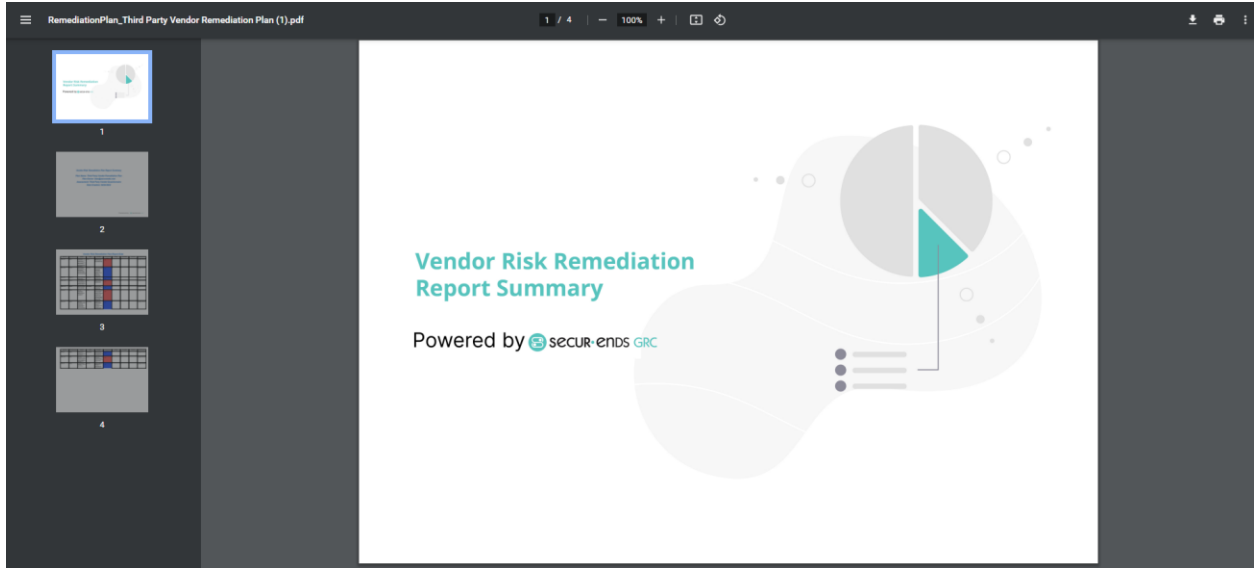
Remediation Plan Generate PDF Back

Remediation Details

Plan Name : Third Party Vendor Remediation Plan  
 Plan Owner : User@securends.com  
 Assessment : Third Party Vendor Questionnaire

Question ID	Presentation Group	Question	Answer	Security Posture Score	Priority	Ticket	Remediation Owner	Risk Remediation
> VenSL77.a	Detect	Does your organization have a process for rout...	1-Initial	20	1	N	User@securends.com	Detected events are analyzed to l
> VenSL3.a	Identify	Do you have an inventory of software within th...	3-Defined	60	1	Y	User@securends.com	Software platforms and applicatic
> VenSL32.a	Protect	Has your organization established an effective ...	1-Initial	20	2	Y	User@securends.com	Access to physical and logical assi
> VenSL33.a	Protect	Does your organization require an authorized ...	2-Repeatable	40	2	Y	User@securends.com	Identities and credentials are issu
> VenSL2.a	Identify	Do you have an inventory of hardware within t...	2-Repeatable	40	2	N	User@securends.com	Physical devices and systems wif
> VenSL110.a	Recover	Do you have a communication plan to manage...	1-Initial	20	3	Y	User@securends.com	Public relations are managed is th
> VenSL111.a	Recover	Does your recovery plans incorporate lessons l...	2-Repeatable	40	3	Y	User@securends.com	Recovery plans incorporate lessor

RemediationPlan\_...pdf Show all





RemediationPlan\_Third Party Vendor Remediation Plan (1).pdf 3 / 4 100%

### Vendor Risk Remediation Plan Report Data

Question Id	Presentation Group	Question	Status	Remediation	Security Posture Score	Priority	Ticket Status	Comments	Remediation Owner
VerSI_95.a	Detect	Do you have processes to detect and alert the incident response team when potential incidents that could lead to data theft or destruction?	1-Initial	Notifications from detection systems are investigated in the expected result.	20	4	N		User@securends.com
VerSI_112.a	Recover	Are processes in place to ensure restored assets are appropriately reconfigured and thoroughly tested, before being placed back into operation?	3-Defined	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events, in the expected result.	60	4	N		User@securends.com
VerSI_97.a	Respond	Do you collect and analyze post-incident evidence?	3-Defined	Forensics are performed in the expected result.	60	4	N		User@securends.com
VerSI_110.a	Recover	Do you have a communication plan to manage public relations and repair reputation after a security breach?	1-Initial	Public relations are managed in the expected result.	20	3	Y		User@securends.com
VerSI_111.a	Recover	Does your recovery plans incorporate lessons learned?	2-Repeatable	Recovery plans incorporate lessons learned in the expected result.	40	3	Y		User@securends.com
VerSI_32.a	Protect	Has your organization established an effective account management processes?	1-Initial	Access to physical and logical assets and associated processes, and devices, and is managed consistent with the assessed risk of unauthorized access, in the expected result.	20	2	Y		User@securends.com
VerSI_33.a	Protect	Does your organization require an authorized user's session to be automatically logged-off after a predetermined period of inactivity?	2-Repeatable	Identifies and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes, in the expected result.	40	2	Y		User@securends.com

## 1.4 Risk Register

Click the **Vendor Risk Management** tab on the main menu and select **Risk Remediation** tab.

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation **Risk Register** Maturity Progress

Risk Register

Search: All Hide/Show Columns Generate PDF Report Save

ID	Source Assessment	Assessment Type	Remediation Date	Question Id	Priority	Presentation Group	Control Set Group	Risk Category	Financial Impact
28	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL32.a	2	Protect	SIGlite-NCSF	Identity Management and A...	Select
29	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL110.a	3	Recover	SIGlite-NCSF	Communications	Select
30	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL77.a	1	Detect	SIGlite-NCSF	Anomalies and Events	Select
31	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL95.a	4	Detect	SIGlite-NCSF	Analysis	Select
32	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL33.a	2	Protect	SIGlite-NCSF	Identity Management and A...	Select
33	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL2.a	2	Identify	SIGlite-NCSF	Asset Management	Select
34	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL111.a	3	Recover	SIGlite-NCSF	Improvements	Select
35	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL112.a	4	Recover	SIGlite-NCSF	Response Planning	Select
36	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL3.a	1	Identify	SIGlite-NCSF	Asset Management	Select
37	Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL97.a	4	Respond	SIGlite-NCSF	Analysis	Select

Rows per page: 10 1-10 of 10

Select **Financial Impact**, **Reputation Impact**, **Mission Impact**, **Assessment Likelihood**, **Exposure Rating** drop-down menus.

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation **Risk Register** Maturity Progress

Risk Register

Search: All Hide/Show Columns Generate PDF Report Save

Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Status
Identity Management and A...	Select	Select	Select	Select	Select	Access to physical and logical assi	User@secureends.com	Select
Communications	Select	Select	Select	Select	Select	Public relations are managed is tr	User@secureends.com	Select
Anomalies and Events	Select	Select	Select	Select	Select	Detected events are analyzed to l	User@secureends.com	Select
Analysis	Select	Select	Select	Select	Select	Notifications from detection syste	User@secureends.com	Select
Identity Management and A...	Select	Select	Select	Select	Select	Identities and credentials are issu	User@secureends.com	Select
Asset Management	Select	Select	Select	Select	Select	Physical devices and systems witt	User@secureends.com	Select
Improvements	Select	Select	Select	Select	Select	Recovery plans incorporate lessor	User@secureends.com	Select
Response Planning	Select	Select	Select	Select	Select	Recovery processes and procedu	User@secureends.com	Select
Asset Management	Select	Select	Select	Select	Select	Software platforms and applicati	User@secureends.com	Select
Analysis	Select	Select	Select	Select	Select	Forensics are performed is the ex	User@secureends.com	Select

Rows per page: 10 1-10 of 10

Select **Status**, **ERM Priority** in drop-down menus and enter **Expected Date**.

SECURE ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

**Risk Register** [Search] All [Hide/Show Columns] [Generate PDF Report] [Save]

act	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Status	Expected Date	ERM Priority
)	Select	Select	Select	Access to physical and logical assi	User@secureends.com	Select		Select
)	Select	Select	Select	Public relations are managed is tr	User@secureends.com	Select		Select
)	Select	Select	Select	Detected events are analyzed to l	User@secureends.com	Select		Select
)	Select	Select	Select	Notifications from detection syste	User@secureends.com	Select		Select
)	Select	Select	Select	Identities and credentials are issu	User@secureends.com	Select		Select
)	Select	Select	Select	Physical devices and systems with	User@secureends.com	Select		Select
)	Select	Select	Select	Recovery plans incorporate lessor	User@secureends.com	Select		Select
)	Select	Select	Select	Recovery processes and procedur	User@secureends.com	Select		Select
)	Select	Select	Select	Software platforms and applicati	User@secureends.com	Select		Select
)	Select	Select	Select	Forensics are performed is the ex	User@secureends.com	Select		Select

Rows per page: 10 1-10 of 10

Select **Hide/Show Columns** in the drop-down menu.

SECURE ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

**Risk Register** [Search] All [Hide/Show Columns] [Generate PDF Report] [Save]

Source Assessment	Assessment Type	Remediation Date	Question Id	Priority	Presentation Group	Control Set Group	Impact	ERM Priority
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_32.a	2	Protect	SIGlite-NCSF	Impact	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_110.a	3	Recover	SIGlite-NCSF	Impact	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_77.a	1	Detect	SIGlite-NCSF	Impact	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_95.a	4	Detect	SIGlite-NCSF	Analysis	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_33.a	2	Protect	SIGlite-NCSF	Identity Management and A...	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_2.a	2	Identify	SIGlite-NCSF	Asset Management	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_111.a	3	Recover	SIGlite-NCSF	Improvements	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_112.a	4	Recover	SIGlite-NCSF	Response Planning	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_3.a	1	Identify	SIGlite-NCSF	Asset Management	Select
Third Party Vendor Remedia...	Internal	Apr 03 2022	VenSL_97.a	4	Respond	SIGlite-NCSF	Analysis	Select

Hide/Show Columns menu:

- ID
- Source Assessment
- Remediation Date
- Question Id
- Priority

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

Risk Register

4 selected

Generate PDF Report Save

Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating
VenSL32.a	2	Protect	Identity Management and A...	Select	Select	Select	Select	Select
VenSL110.a	3	Recover	Communications	Select	Select	Select	Select	Select
VenSL77.a	1	Detect	Anomalies and Events	Select	Select	Select	Select	Select
VenSL95.a	4	Detect	Analysis	Select	Select	Select	Select	Select
VenSL33.a	2	Protect	Identity Management and A...	Select	Select	Select	Select	Select
VenSL2.a	2	Identify	Asset Management	Select	Select	Select	Select	Select
VenSL111.a	3	Recover	Improvements	Select	Select	Select	Select	Select
VenSL112.a	4	Recover	Response Planning	Select	Select	Select	Select	Select
VenSL3.a	1	Identify	Asset Management	Select	Select	Select	Select	Select
VenSL97.a	4	Respond	Analysis	Select	Select	Select	Select	Select

Rows per page: 10 1-10 of 10

Click the **Save** button.

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

Risk Register

4 selected

Generate PDF Report Save

ID	Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating
21	VenSL110.a	2	Recover	Communications	Low	Low	Low	Low	2

Generate Remediation Plan Report

Click the **Generate PDF Report** button.

Vendor Risk Management

Dashboard Assessment Campaigns Assessment Reports Risk Report Risk Remediation Risk Register Maturity Progress

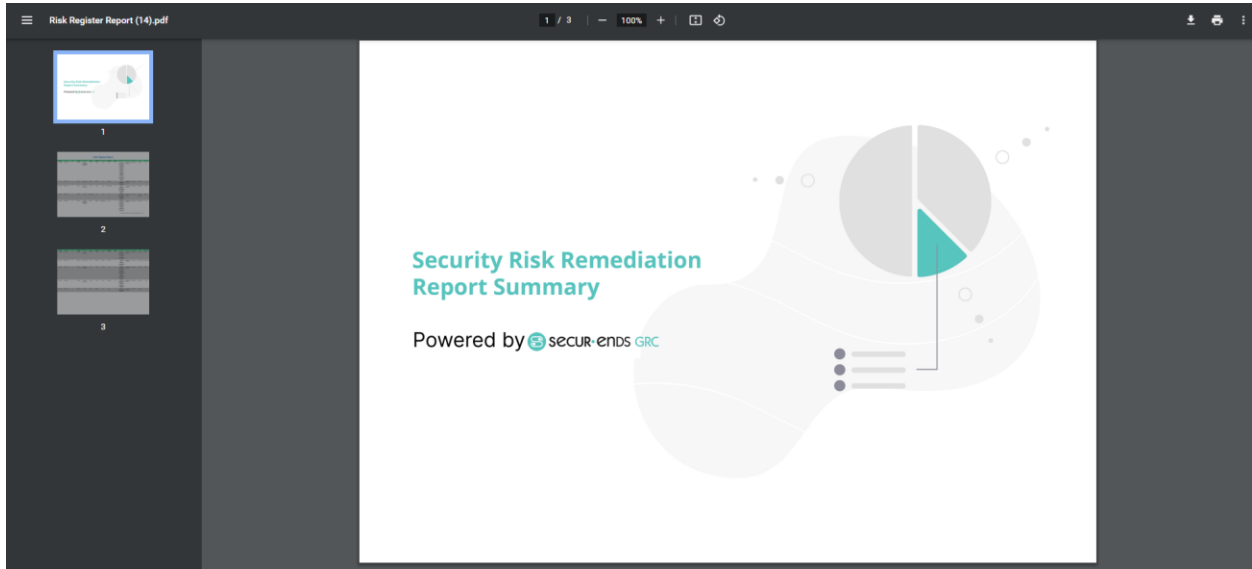
Risk Register

4 selected

Generate PDF Report Save

ID	Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating
21	VenSL110.a	2	Recover	Communications	Low	Low	Low	Low	2
22	VenSL81.a	4	Detect	Security Continuous Monitor...	Medium	High	Medium	Medium	8
23	VenSL2.a	2	Identify	Asset Management	Not Available	Medium	Medium	Medium	5

Open or Save PDF Report as available through the browser.



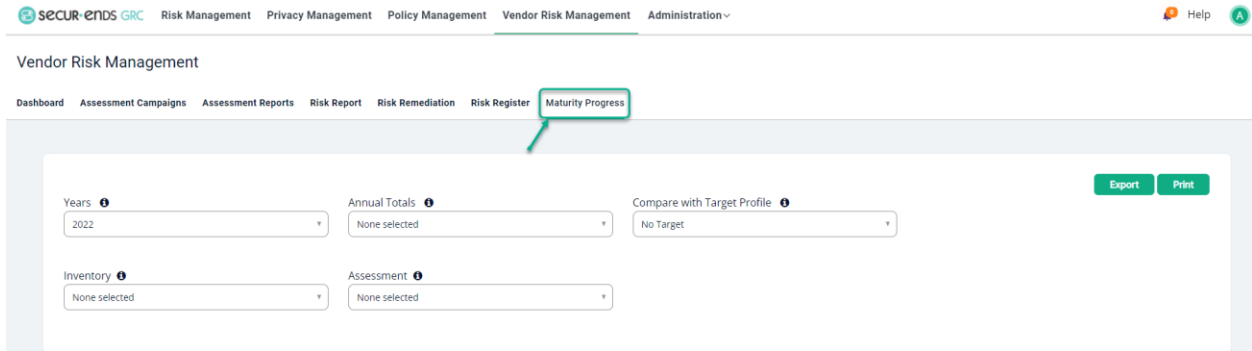
Risk Register Report

Assessment Type	Question Id	Priority	Presentation Style	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Expected Date	Status	ERM Priority
Internal	VerSL32.a	2	Protect	Identity Management and Access Control	Low	Low	Low	Low	6	Access to physical and logical assets associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. Is the expected result.	User@secure-ends.com	2022-04-29	Pending	Low
Internal	VerSL110.a	3	Recover	Communications	Medium	Medium	Low	Medium	1	Public relations are managed in the expected result.	User@secure-ends.com	2022-04-30	Completed	Low
Internal	VerSL77.a	1	Detect	Anomalies and Events	High	High	High	Not Applicable	10	Detected events are analyzed to understand attack targets and methods in the expected result.	User@secure-ends.com	2022-04-22	Completed	High
Internal	VerSL35.a	4	Respond	Analysis	Not Applicable	Low	Low	Low	5	Notifications from detection systems are investigated in the expected result.	User@secure-ends.com	2022-04-28	No Actions Required	Medium
Internal	VerSL33.a	2	Protect	Identity Management and Access Control	Medium	Medium	Not Applicable	High	7	Identifies and credentials are issued, reviewed, and audited for authorized devices, users, and processes in the expected result.	User@secure-ends.com	2022-04-26	In Progress	Low

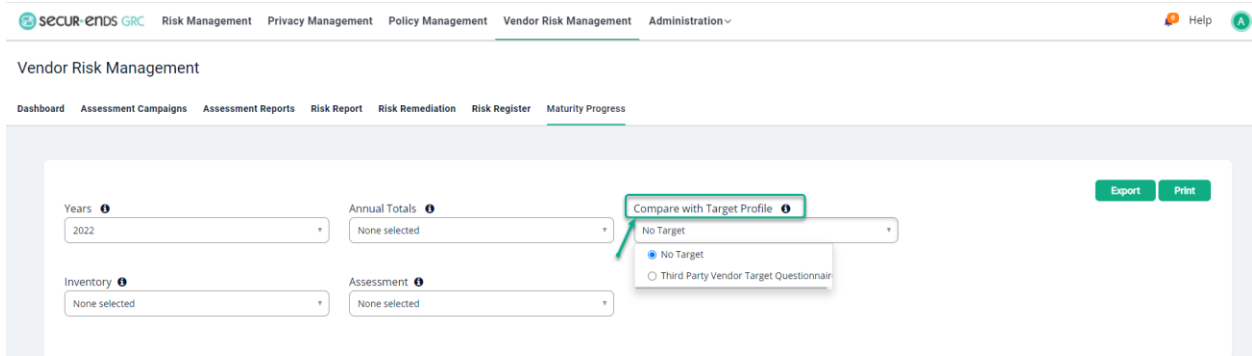
Powered by secur-ends GRC

## 1.5 Maturity Progress

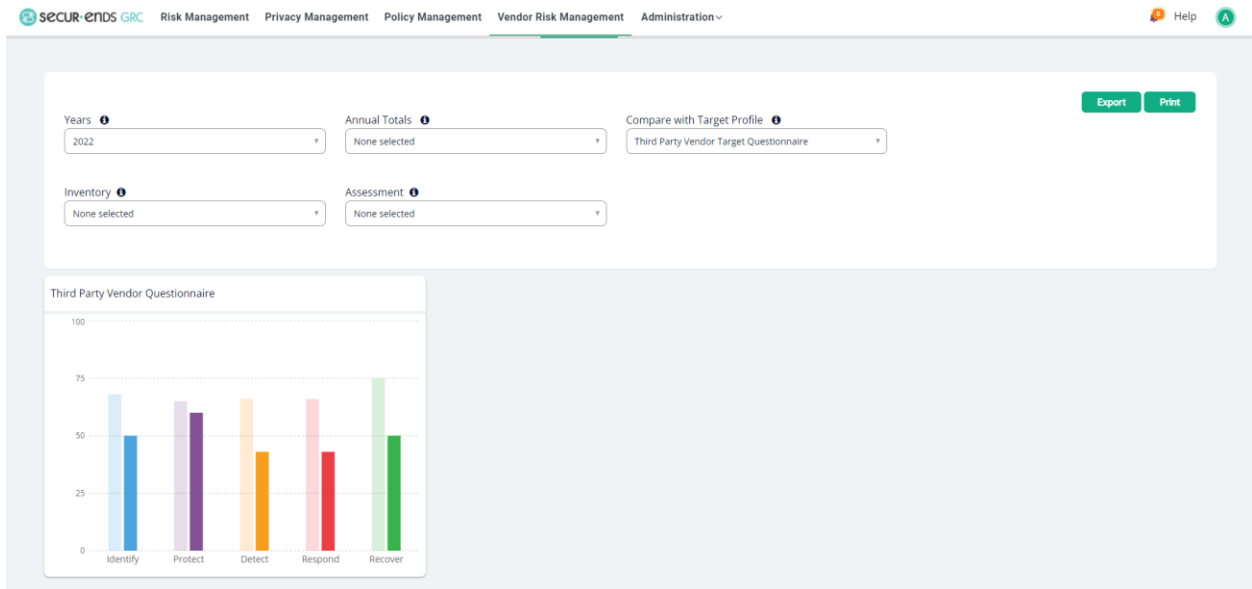
Click the **Vendor Risk Management** tab on the main menu and select **Maturity Progress** tab.



Select **Target Profile** from the drop-down menu to compare with the Campaigns.



Select **Years/ Annual totals / Inventory/ Assessment**.



[End of Vendor Management User Guide]