2022

Vendor Risk Management

User Guide

Table of Contents

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

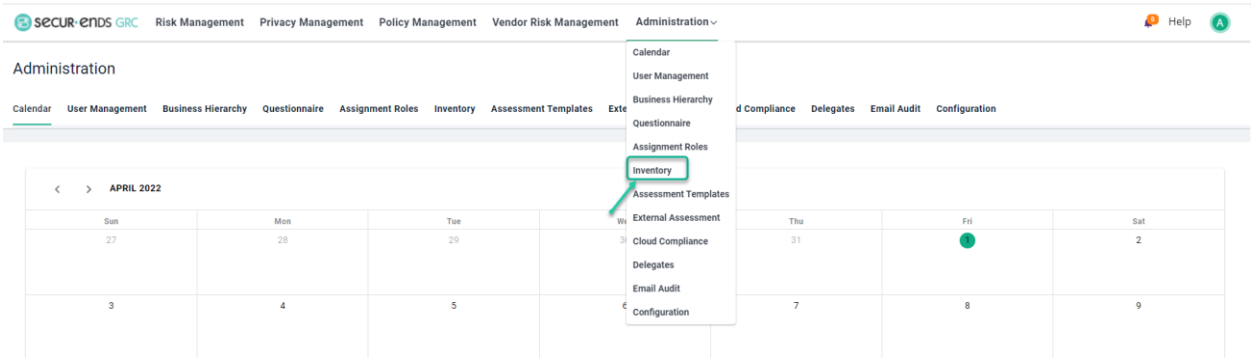
An easy user interface to drive adoption in the assessment process for third party vendors. Standardized formats to increase success in managing vendors, partners, service providers, and more.

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

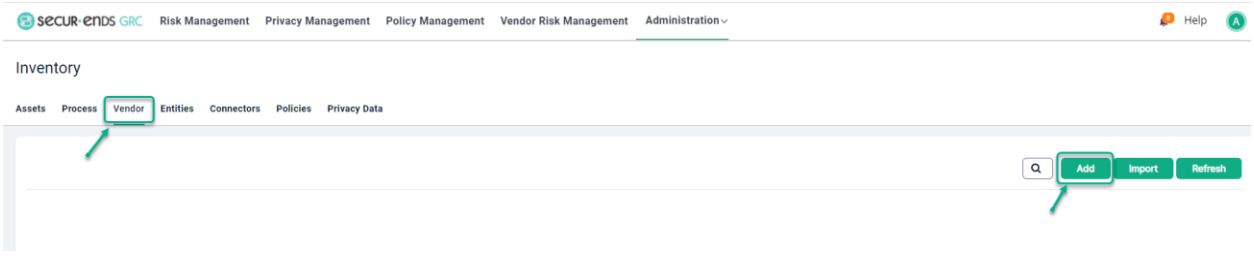
Note: For Vendor Risk Management select Vendor in Inventory.

Add a Vendor under the Inventory.

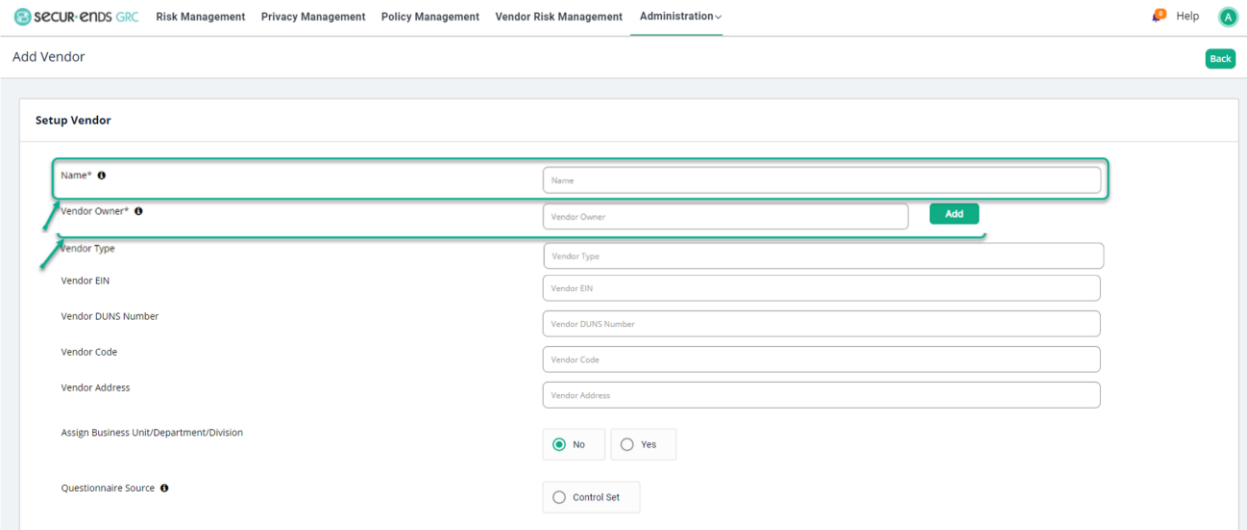
Select the **Inventory** option in **Administration** drop-down list.



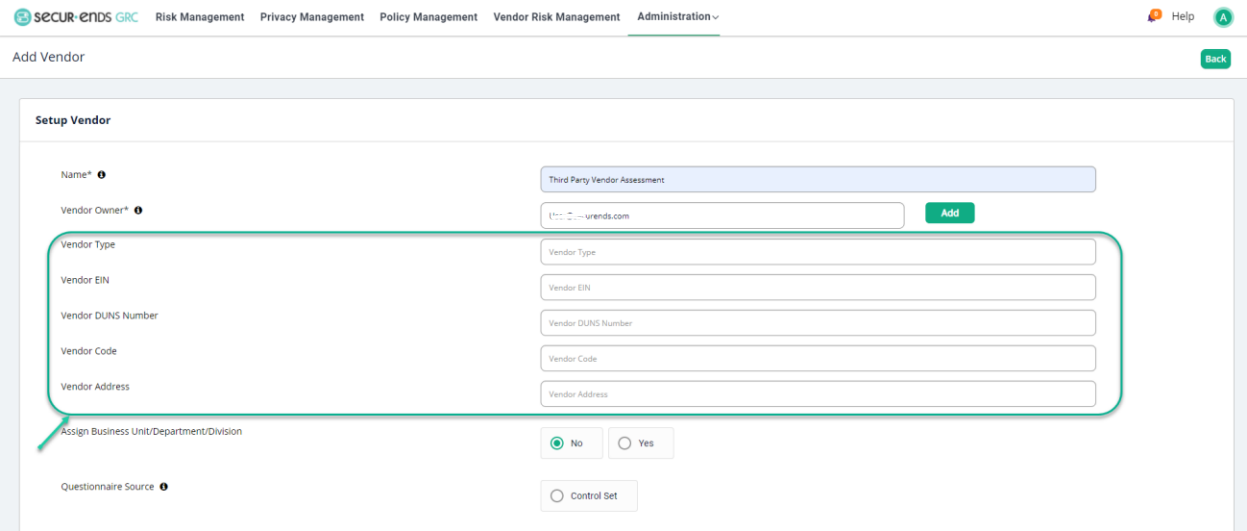
Select **Vendor** and click the **Add** button.



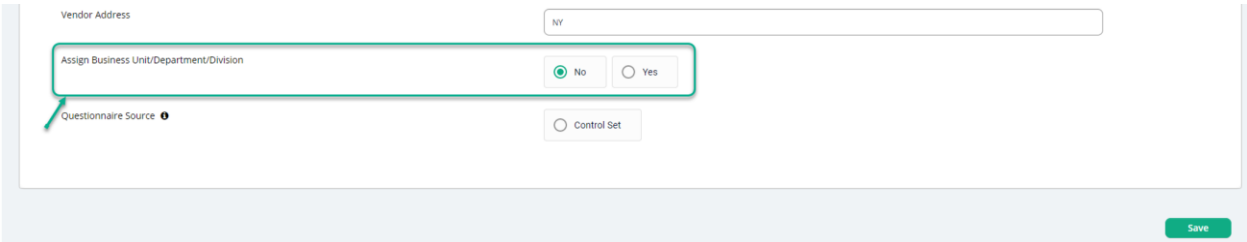
Name the Vendor and then assign a **Vendor Owner** (by selecting the user in the contacts or add new user as appropriate).



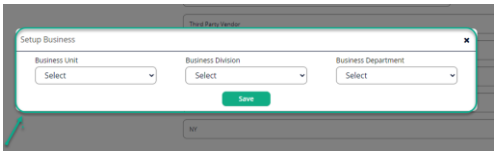
Enter **Vendor Type**, **Vendor EIN**, **Vendor DUNS Number**, **Vendor Code** and **Vendor Address.**



Assign it to a level within the Business Hierarchy.



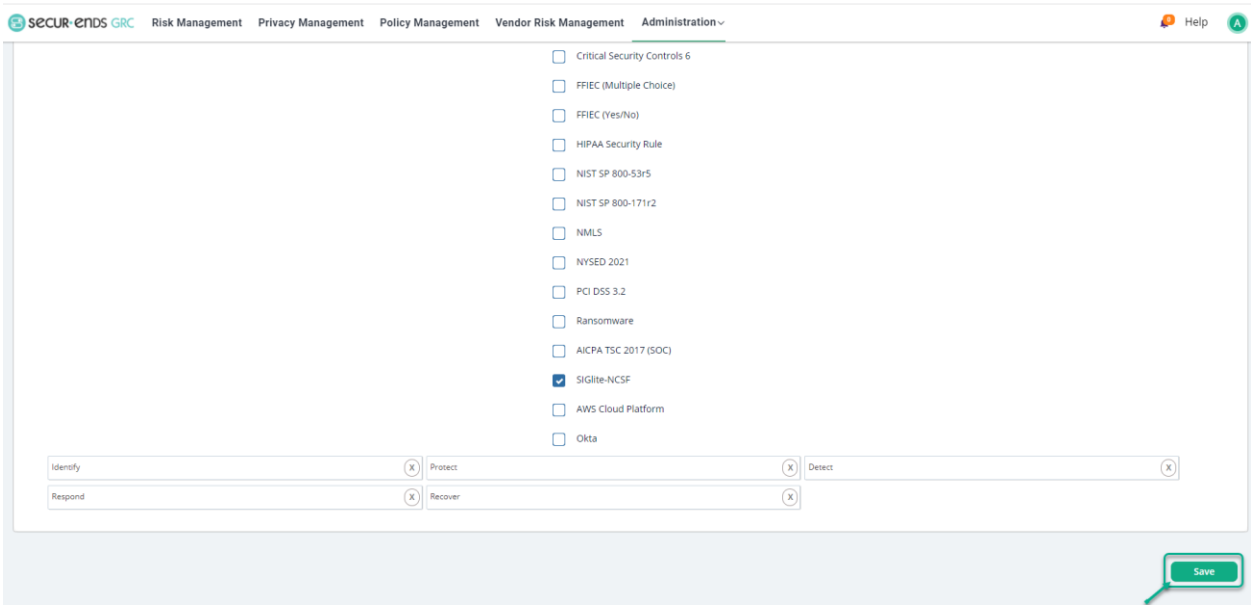
Select the **Yes** radio button and assign it to a business level and click the **Save** button.



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

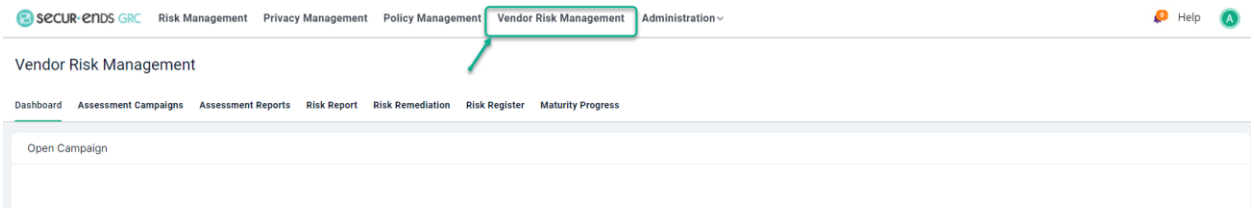
Select box for **SIGlite-NCSF.**

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

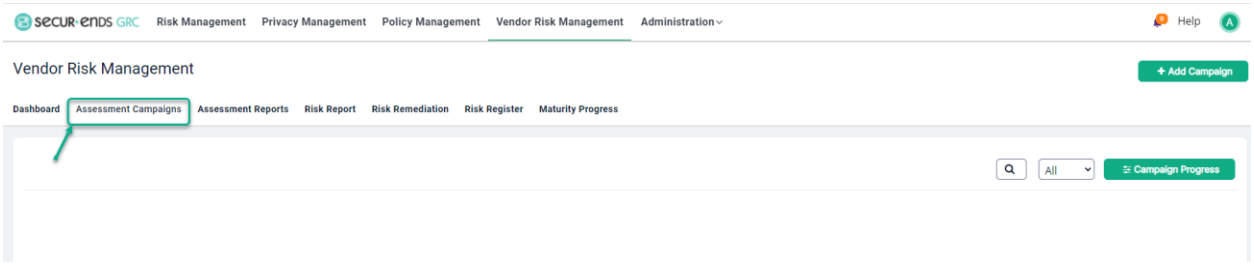


1.1 Assessment Campaigns

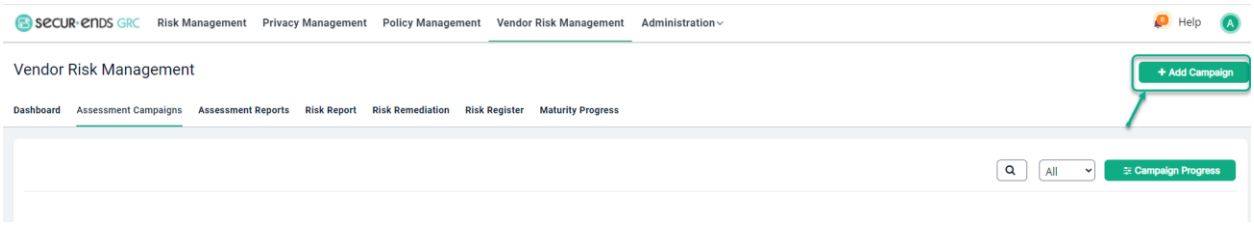
Select the **Vendor Risk Management** tab on the main menu.



Select **Assessment Campaigns** Tab.



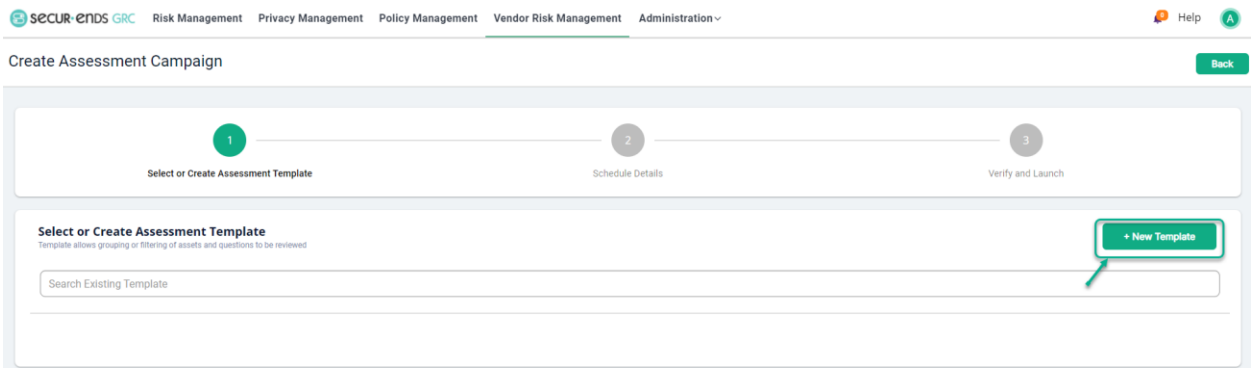
Click the **Add Campaign** button to follow three step process.



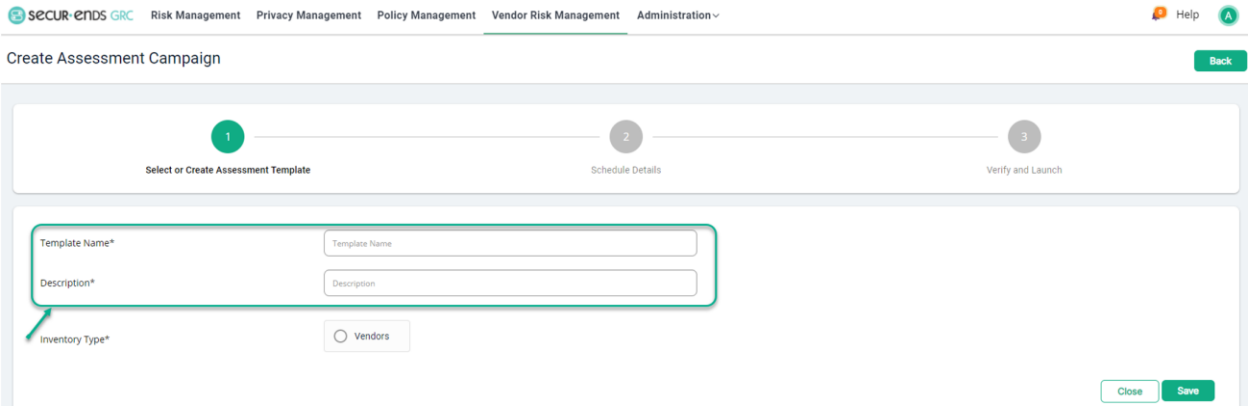
The three-step process page is launched.

1.1.1 Step 1: Select or Create Assessment Template.

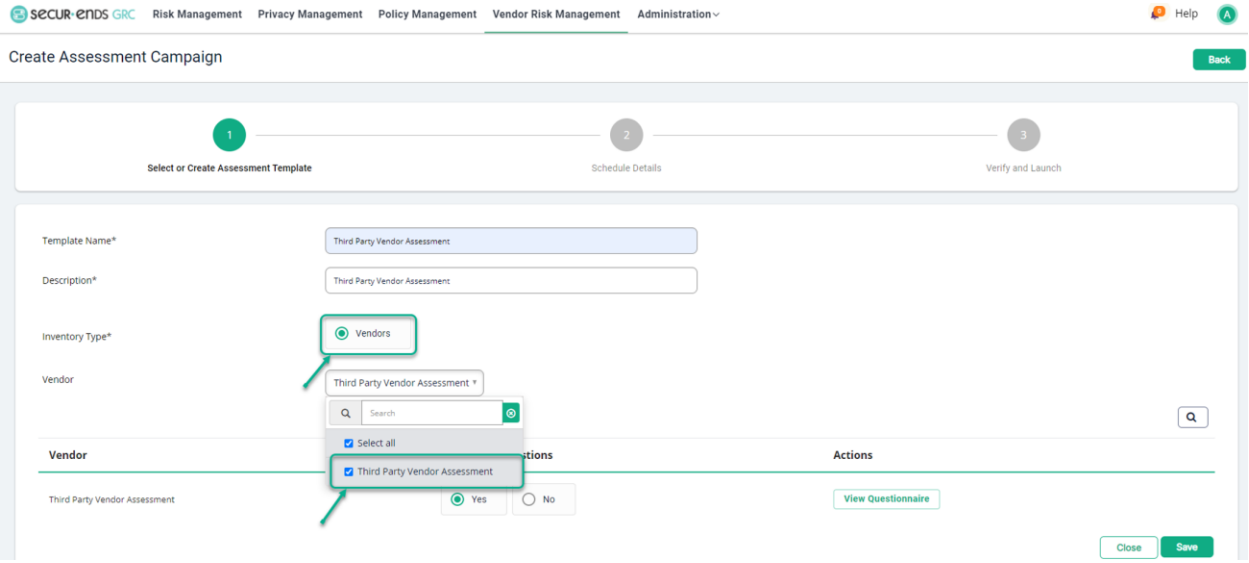
Click the **New Template** button to create new Assessment Template.



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

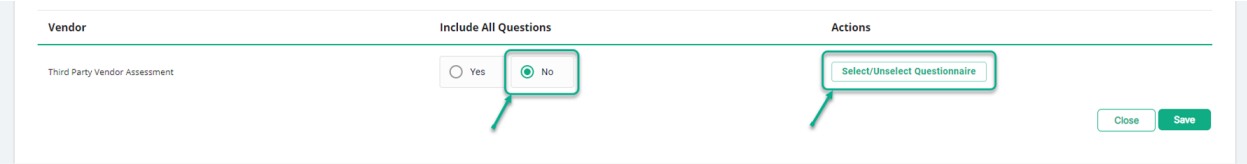


Click the **Vendors** radio button and select the Vendor from the dropdown list.

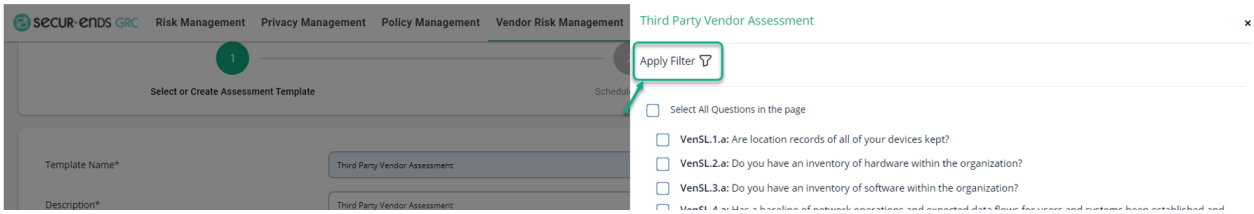


Click the **Yes** radio button to select all questions.

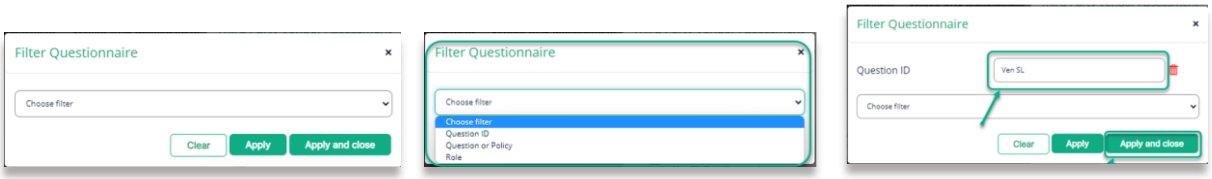
Or, click the **No** radio button and then click the **Select/Unselect Questionnaire** button.



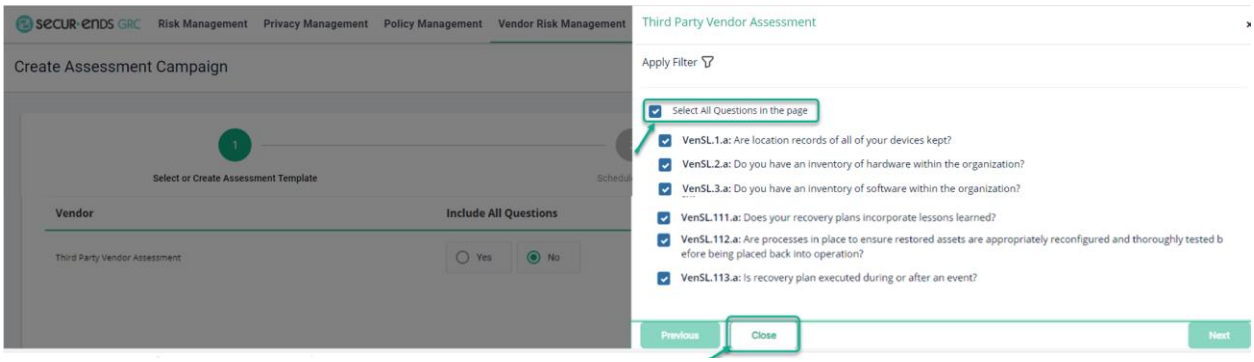
Click the **Apply Filter** symbol.



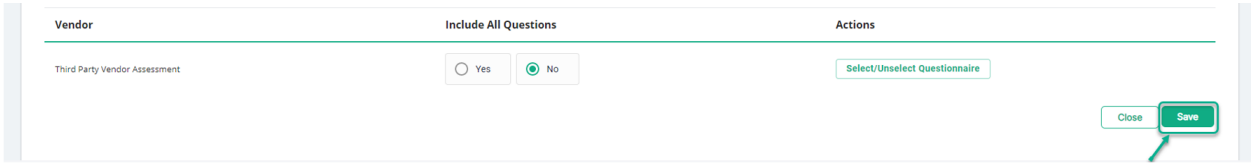
At the pop-up window, choose Filter **Question ID**/ **Question or Policy** / **Role.** Enter Question ID and then click on **Apply and Close** button.



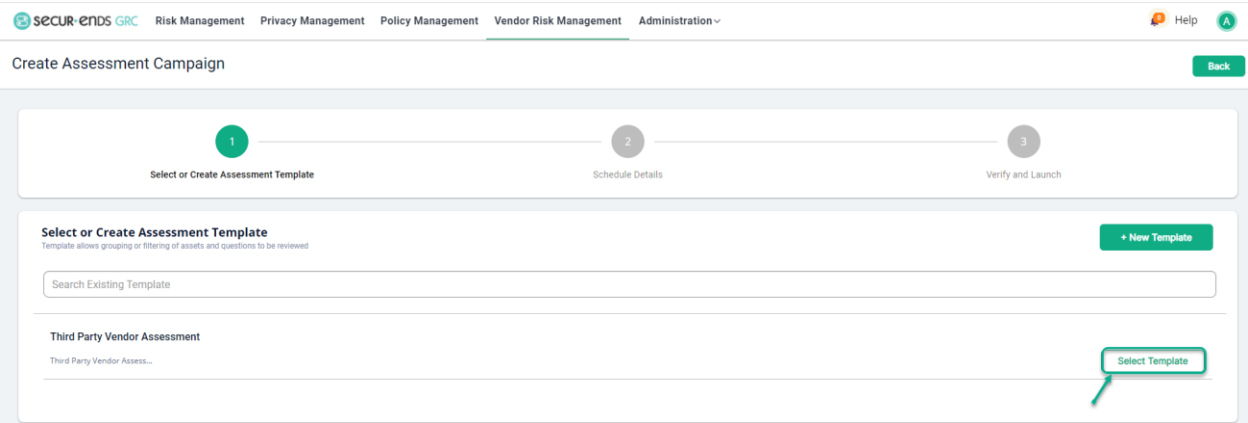
Check the box for **Select All Questions** in the page and click the **Close** button.



Click the **Save** button.



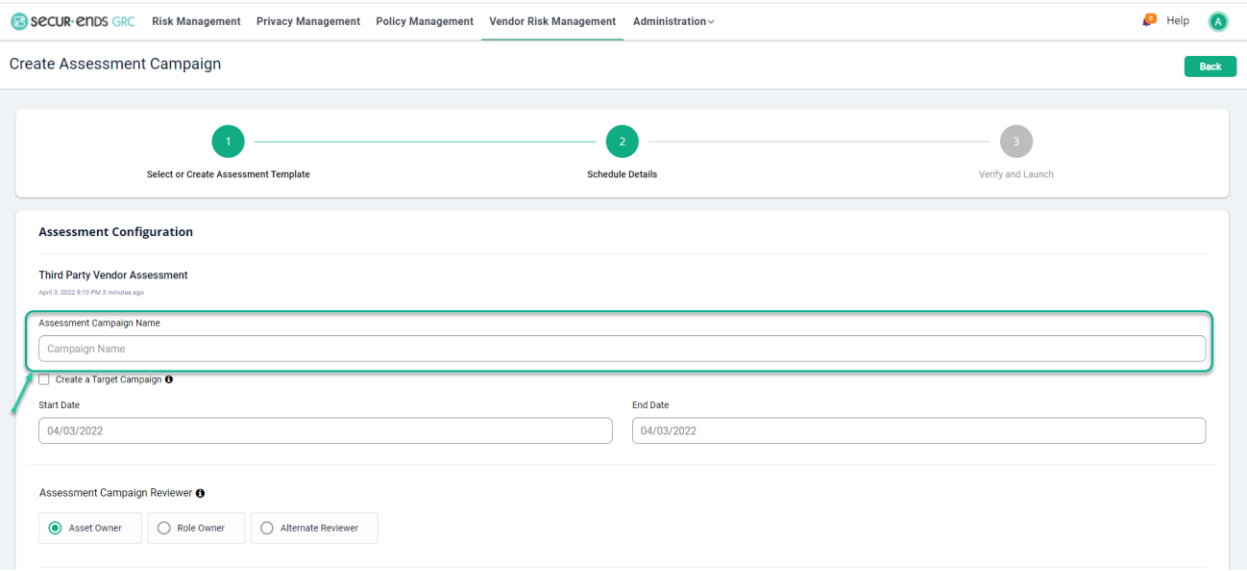
Select the Assessment Template that was created.



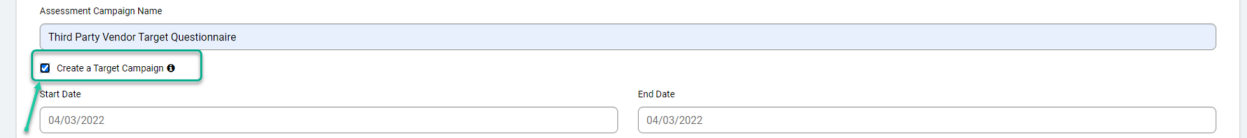
1.1.2 Step 2: Schedule Details

Assessment Configuration

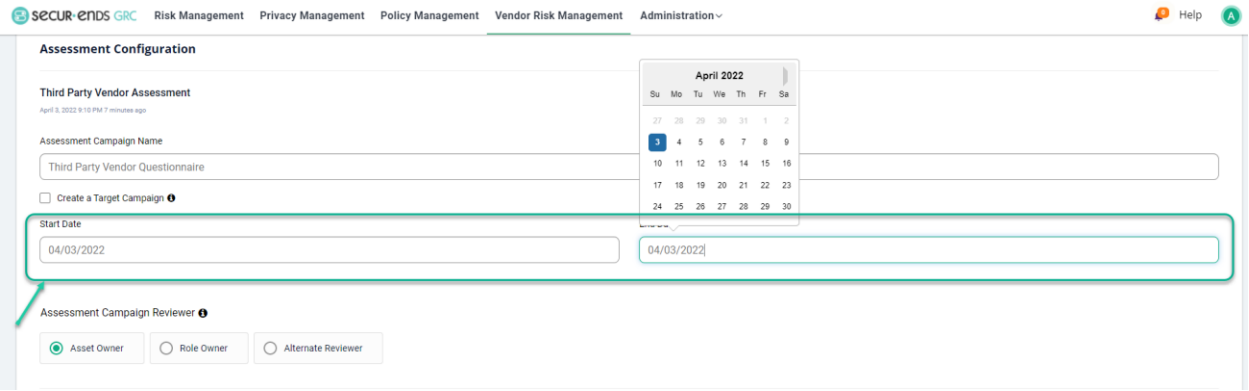
Enter Assessment Campaign Name.



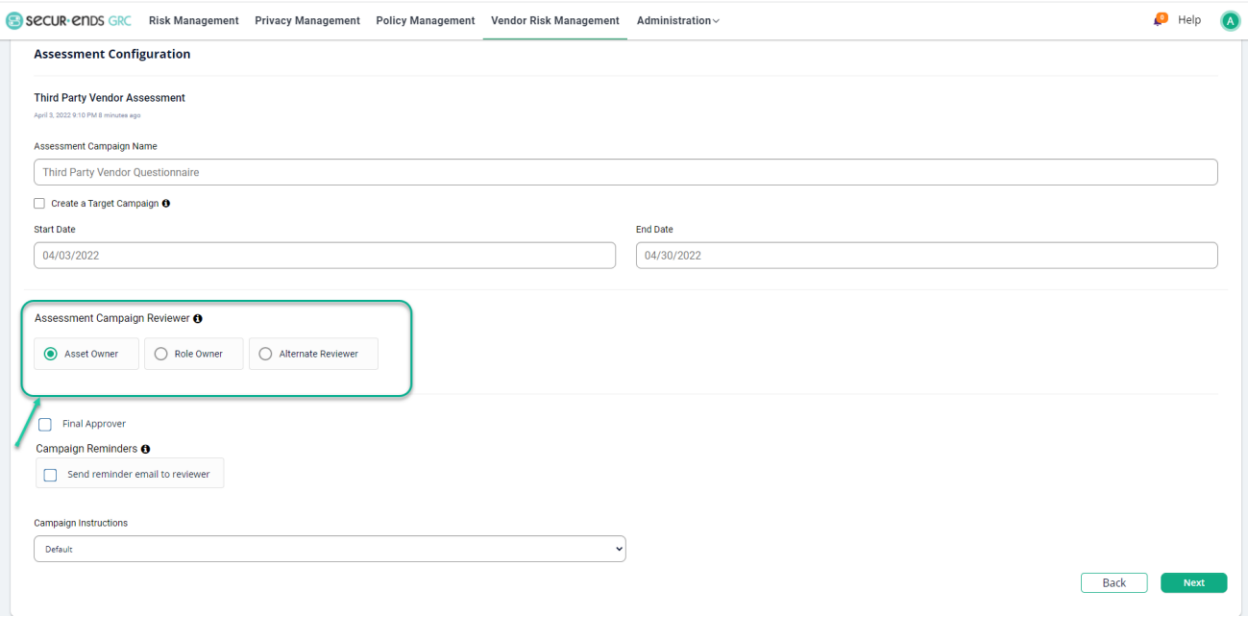
Note: For creating Target Campaign select “Create a Target Campaign” option and enter Alternate Reviewer.



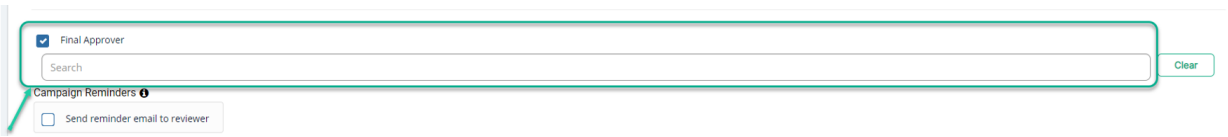
Select a “Start Date” and “End Date”.



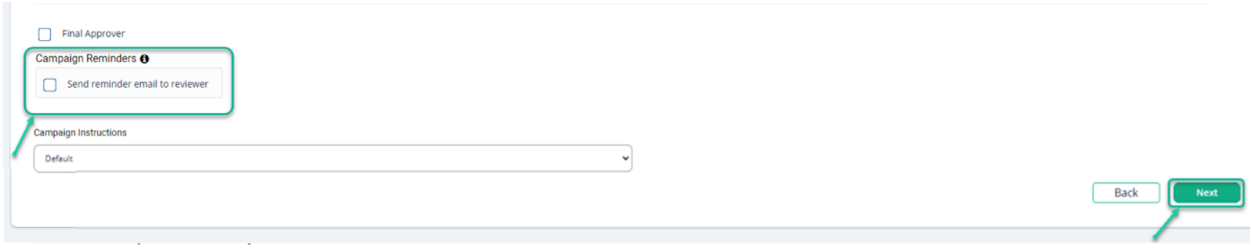
Select **Asset Owner/Role owner/Alternate Reviewer.**



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

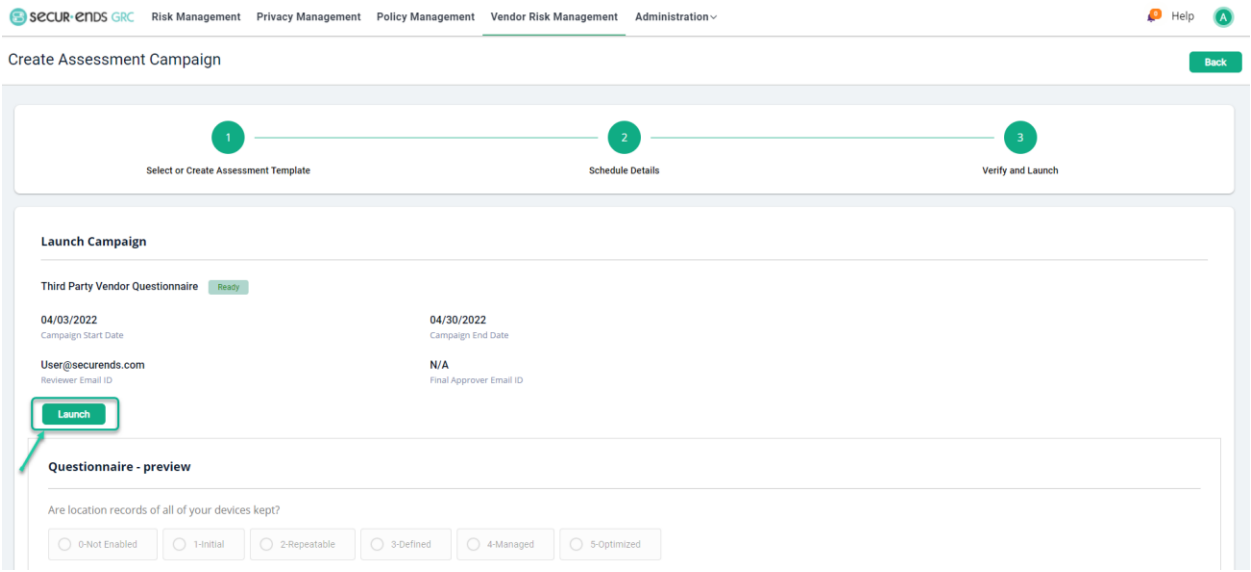


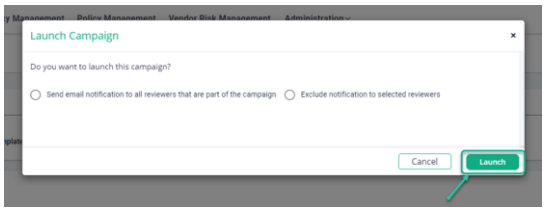
Select **Campaign Reminders** option (By selecting this option, the reminder email can send to Reviewer). The **Campaign Instructions** dropdown menu provides the option for the administrator to change the default message at the top of the campaign to a note or instructions for the reviewer. Click the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



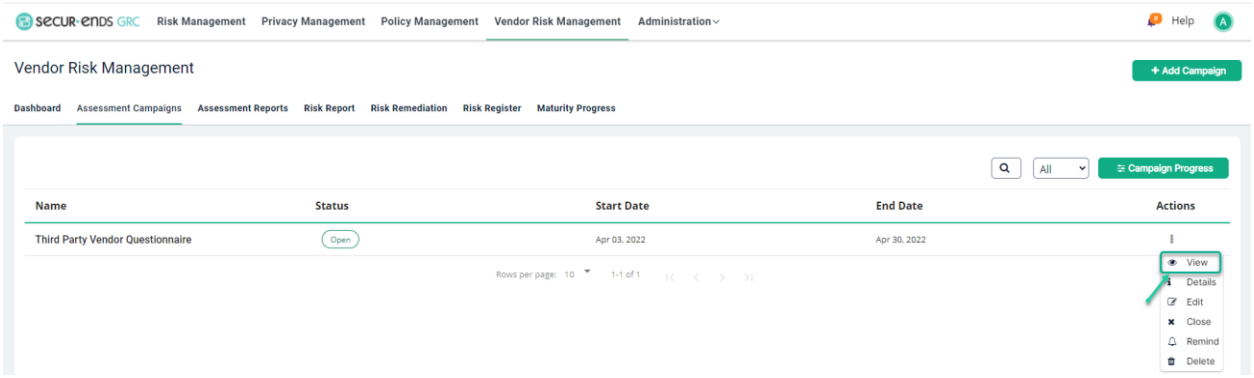
1.1.3 Step 3: Verify and Launch.

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

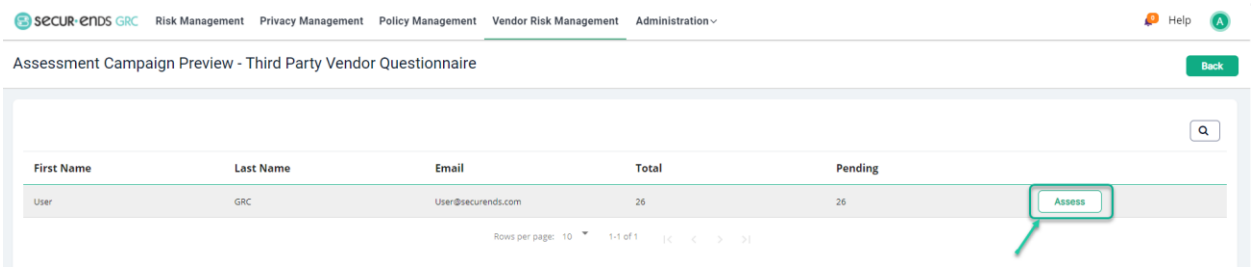




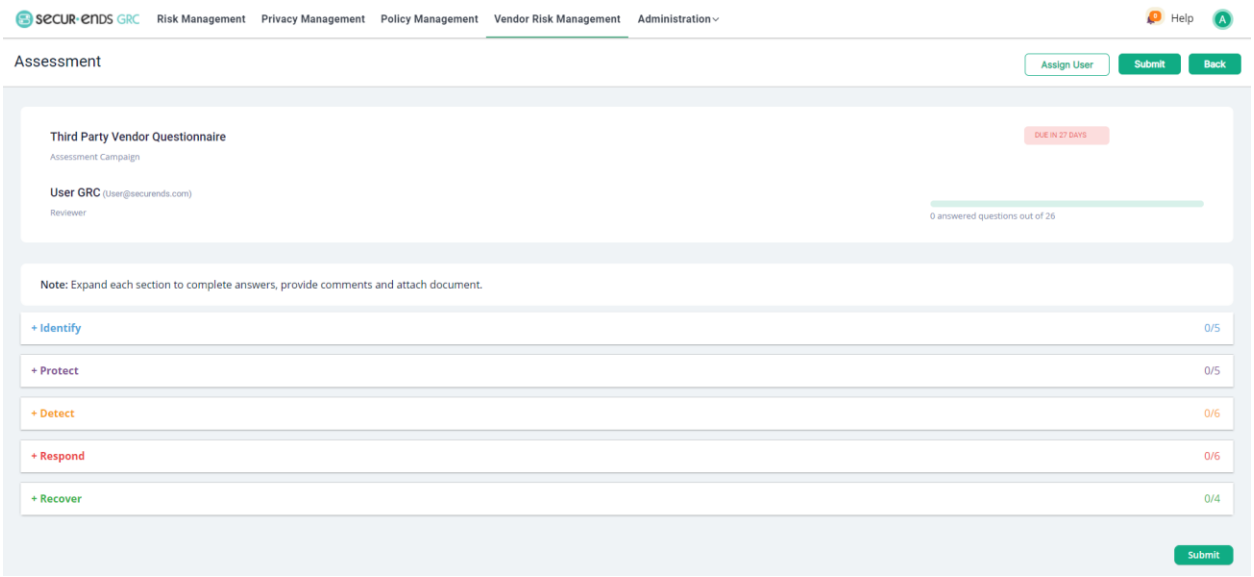
Open the Actions menu and select View item.



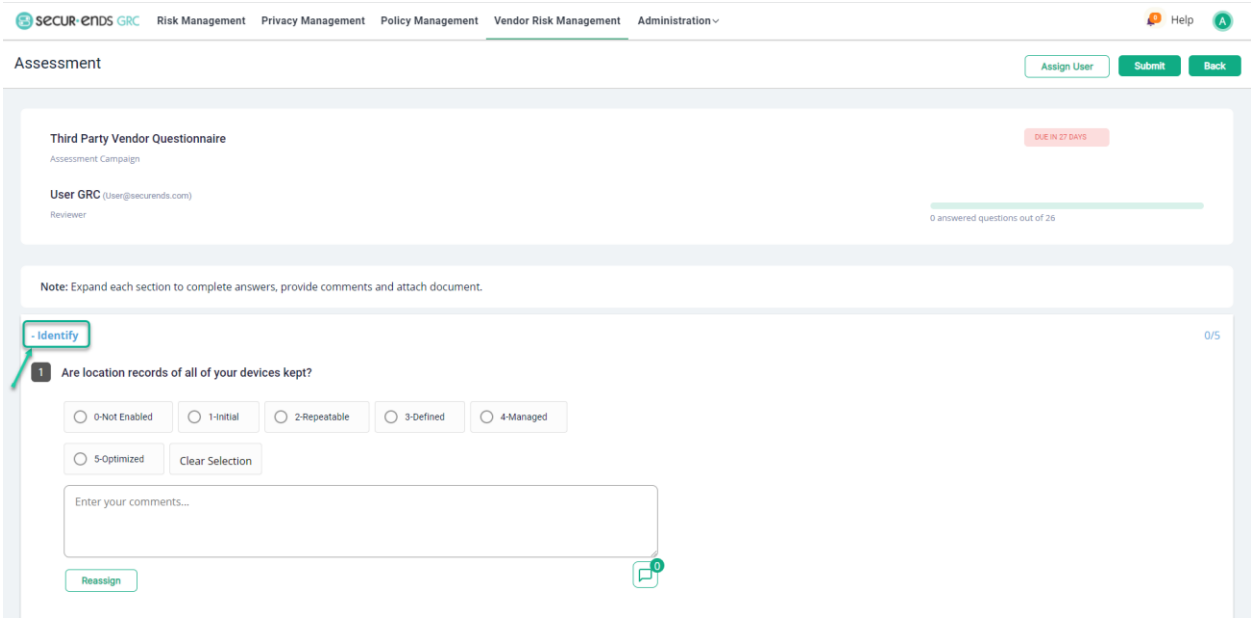
On the Assessment Campaign Preview page, select the Assess button on the right.



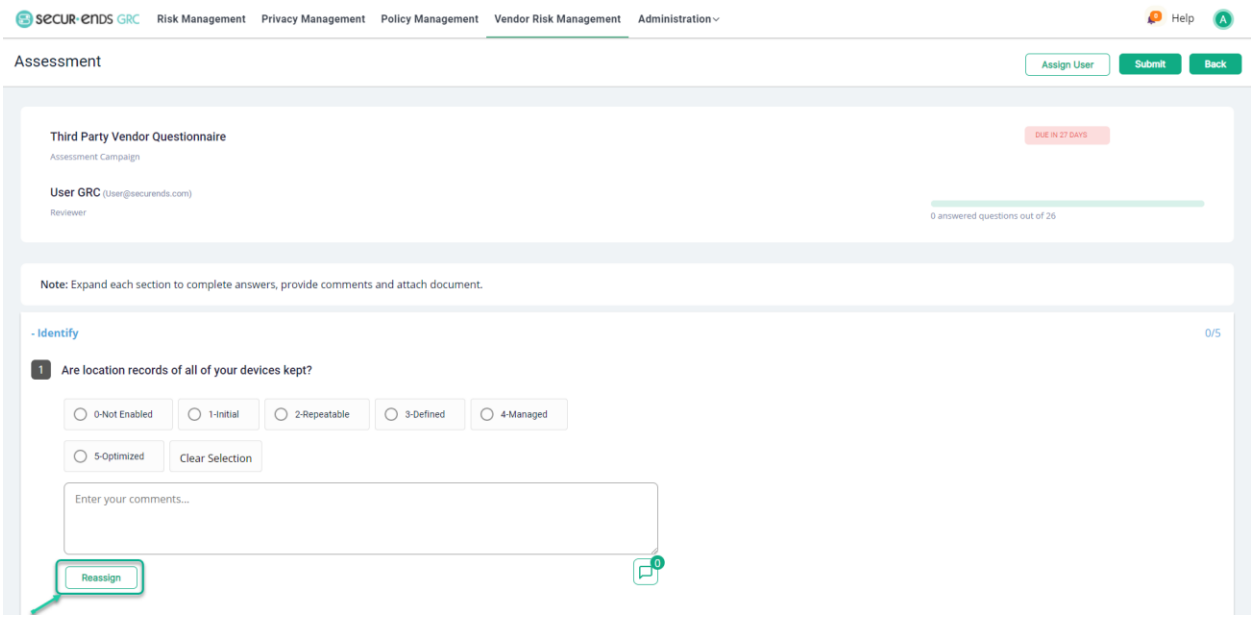
The user is presented with the outline of the assessment.



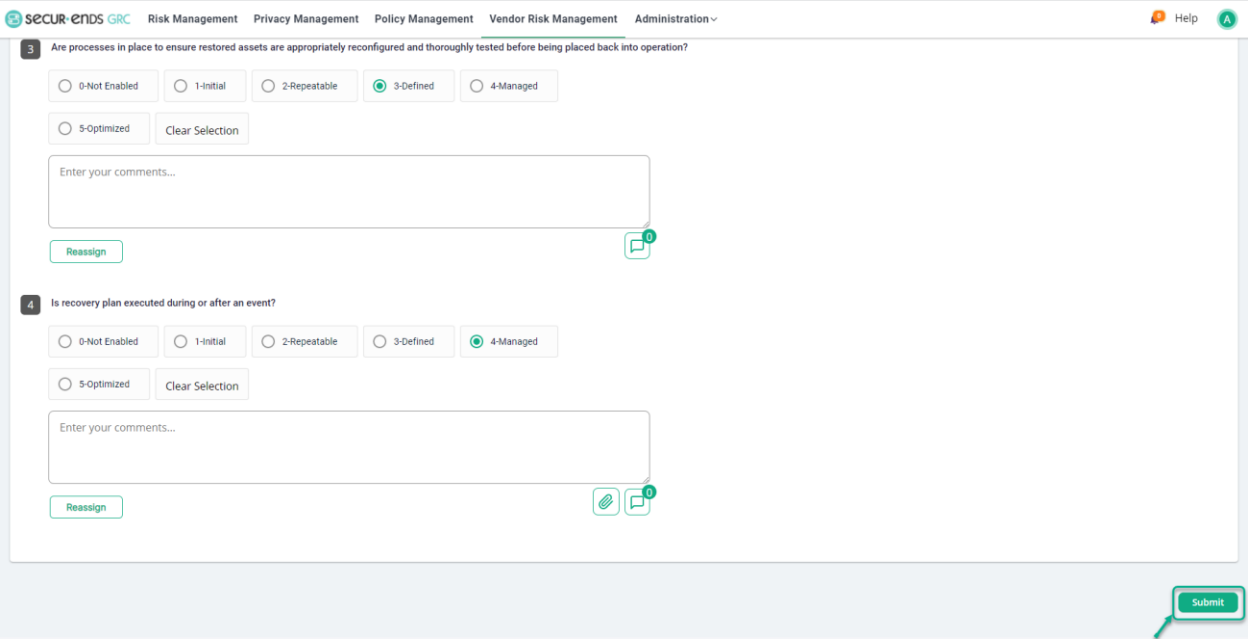
Expand each section to complete answers, provide comments and attach document.



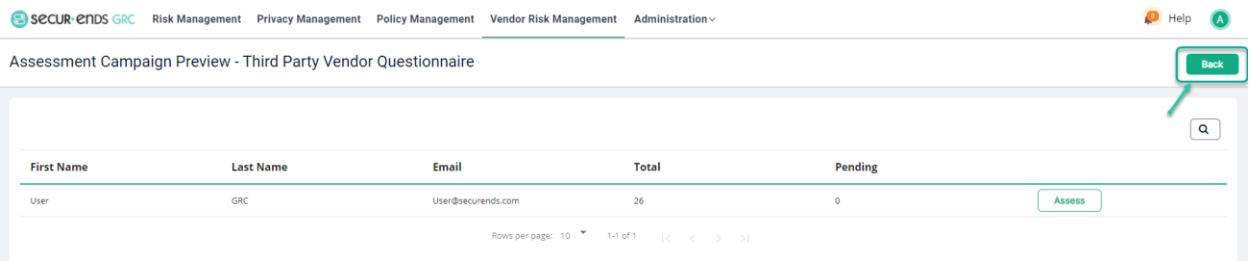
Select **Reassign** button (by selecting this option can reassign the question to another reviewer).



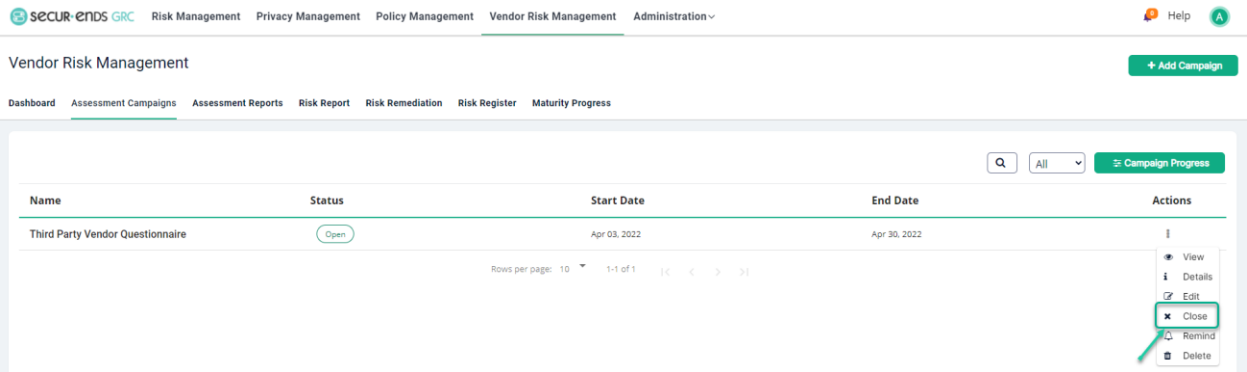
Answer all questions and click the **Submit** button.



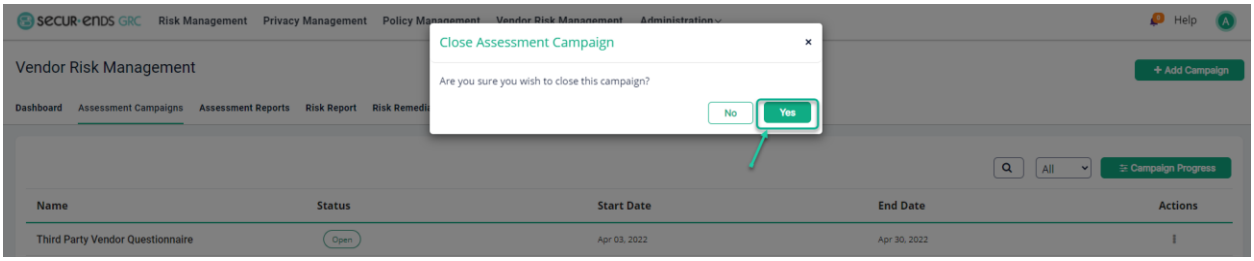
Click the **Back** button.

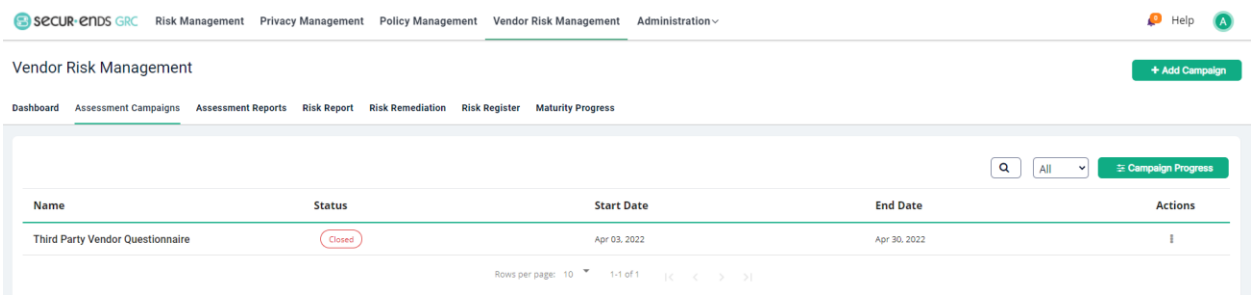


Click the Actions menu and select **Close** option to close the campaign.



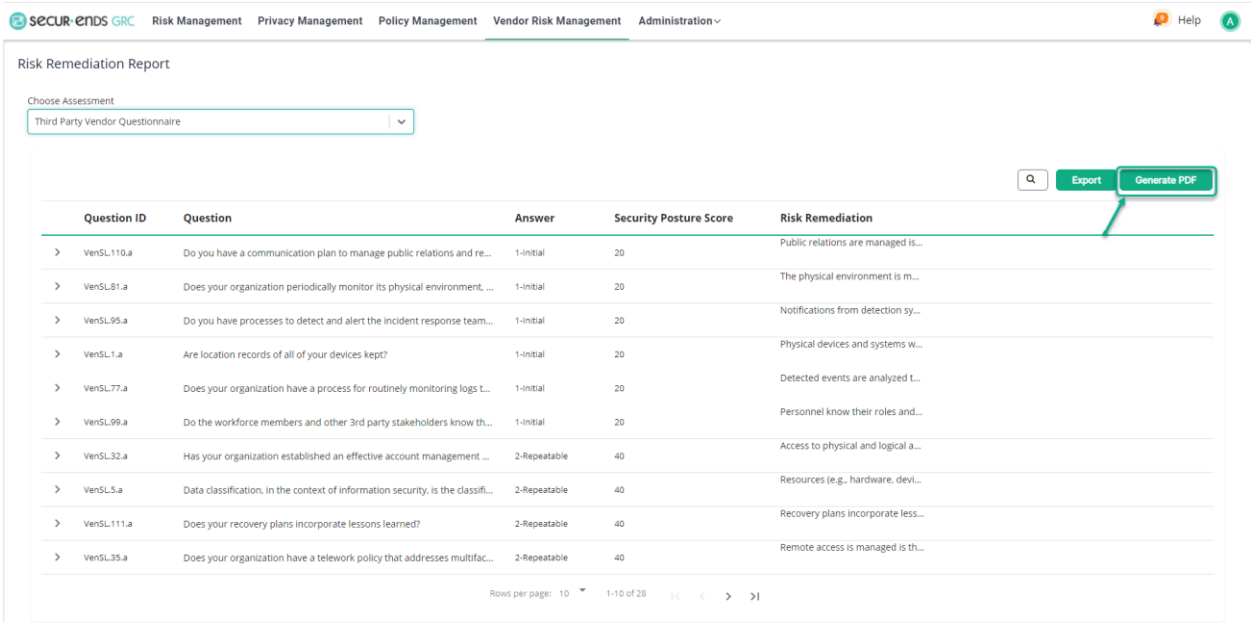
Select **Yes** option to close the Campaign.



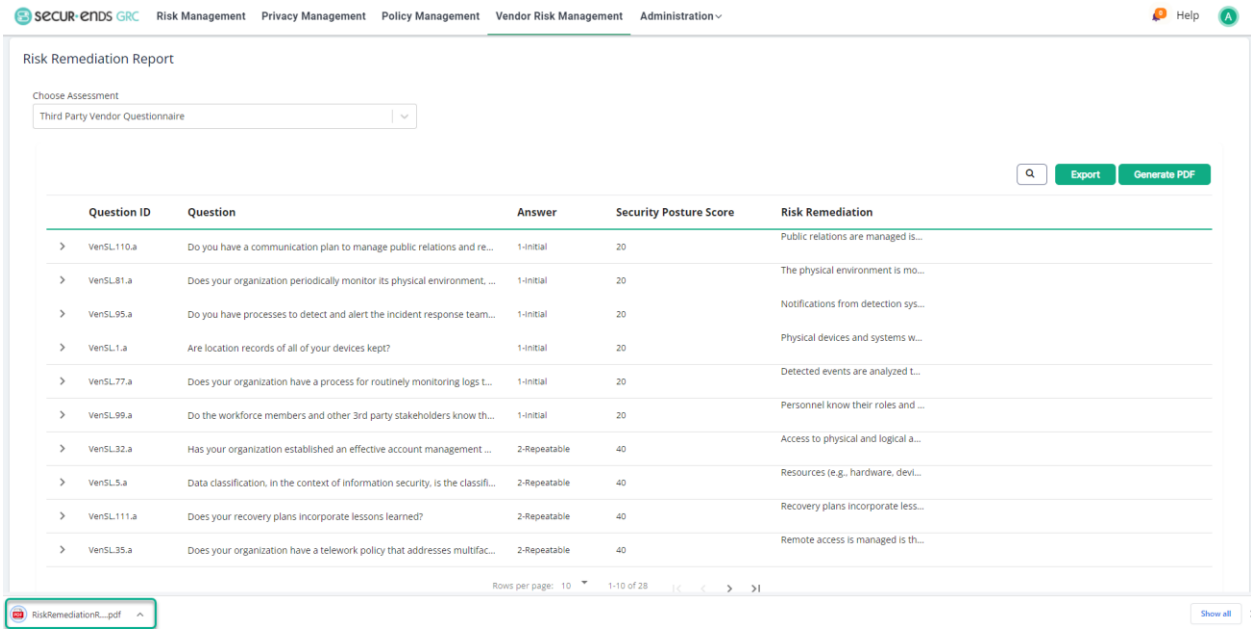


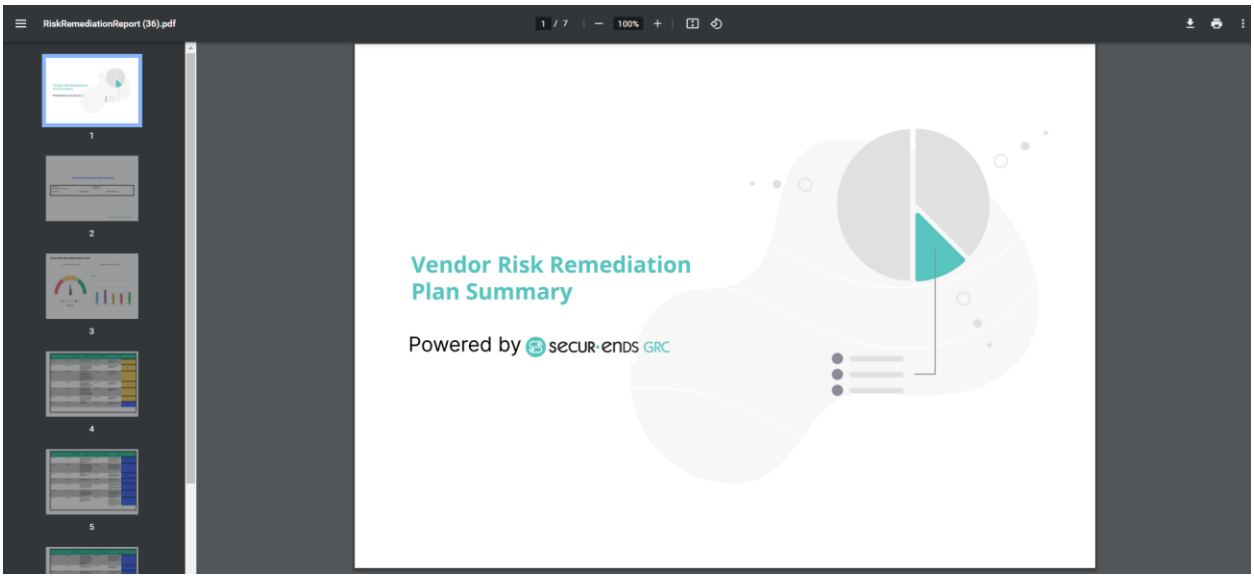
1.2 Risk Report

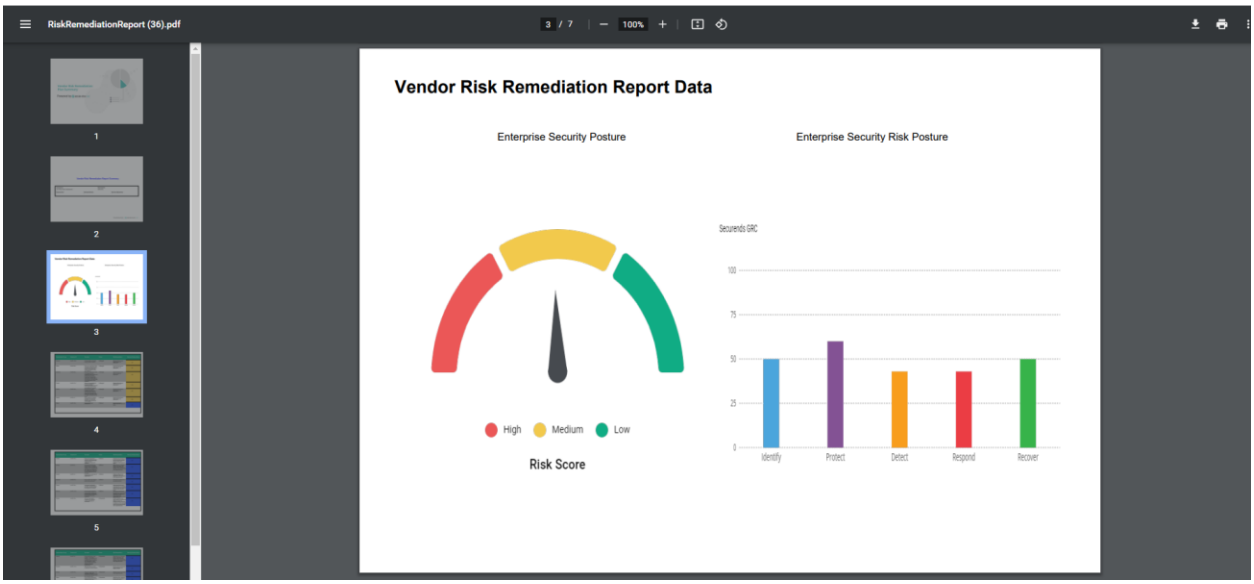
Click the **Generate PDF** button to generate Risk Remediation PDF Report.

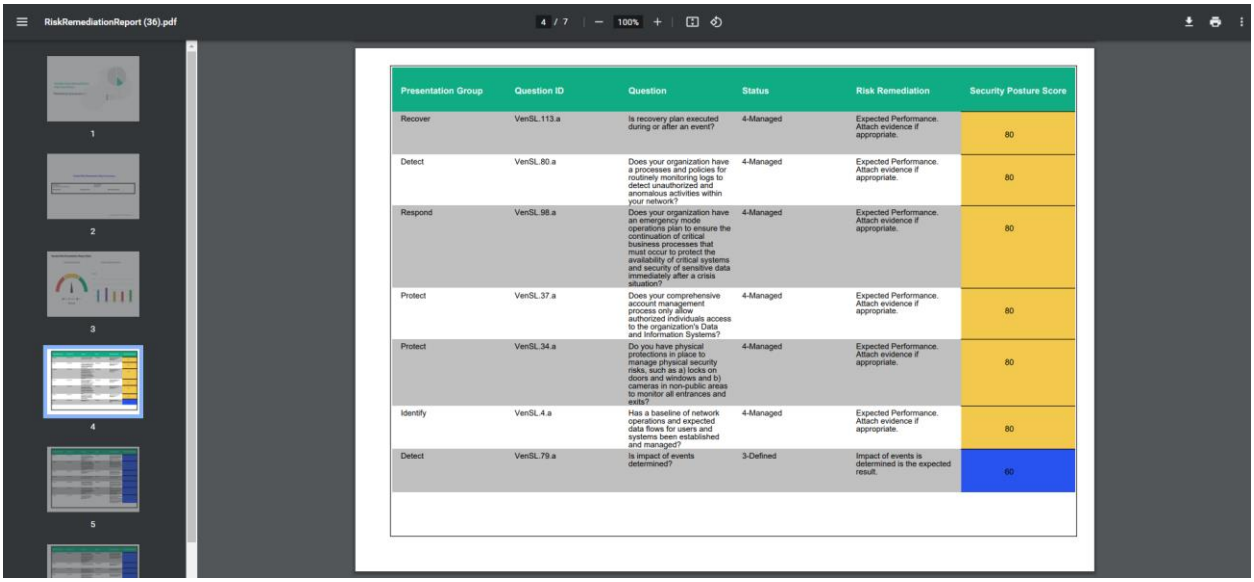


Open or Save the PDF as supplied through the browser interface.







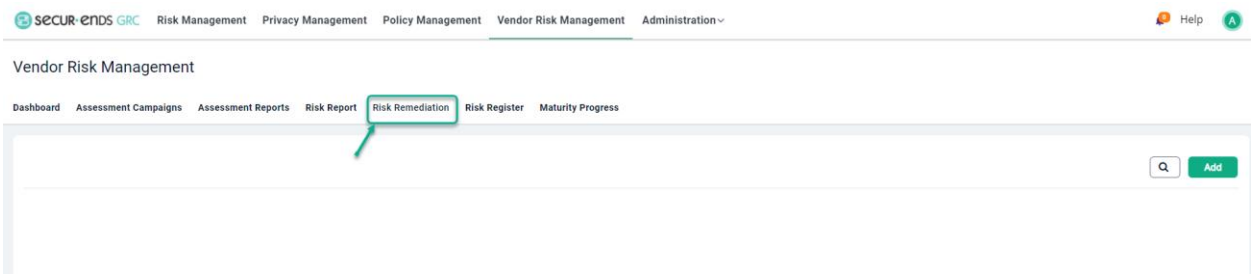


Presentation Group	Question ID	Question	Status	Risk Remediation	Security Posture Score
Recover	VenSL.113.a	Is recovery plan executed during or after an event?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Detect	VenSL.80.a	Does your organization have a processes and policies for routinely monitoring logs to detect unauthorized and anomalous activities within your network?	4-Managed	Expected Performance. Attach evidence if appropriate.	80
Respond	VenSL.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	VenSL.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	VenSL.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	VenSL.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	VenSL.79.a	Is impact of events determined?	3-Defined	Impact of events is determined is the expected result.	60

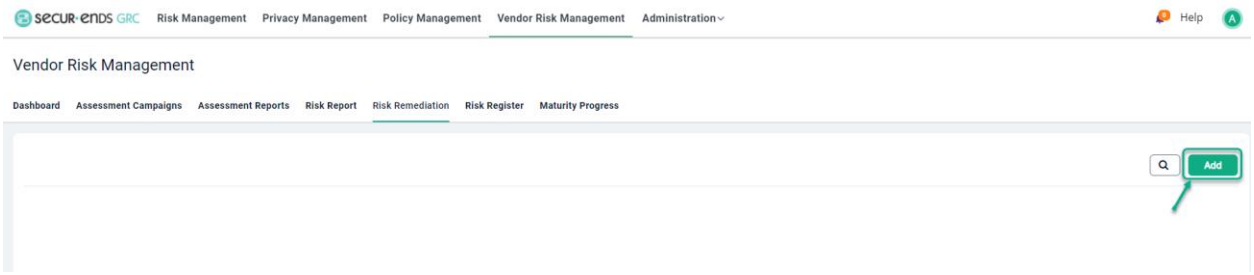
1.3 Risk Remediation

Creation of Remediation Plan.

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

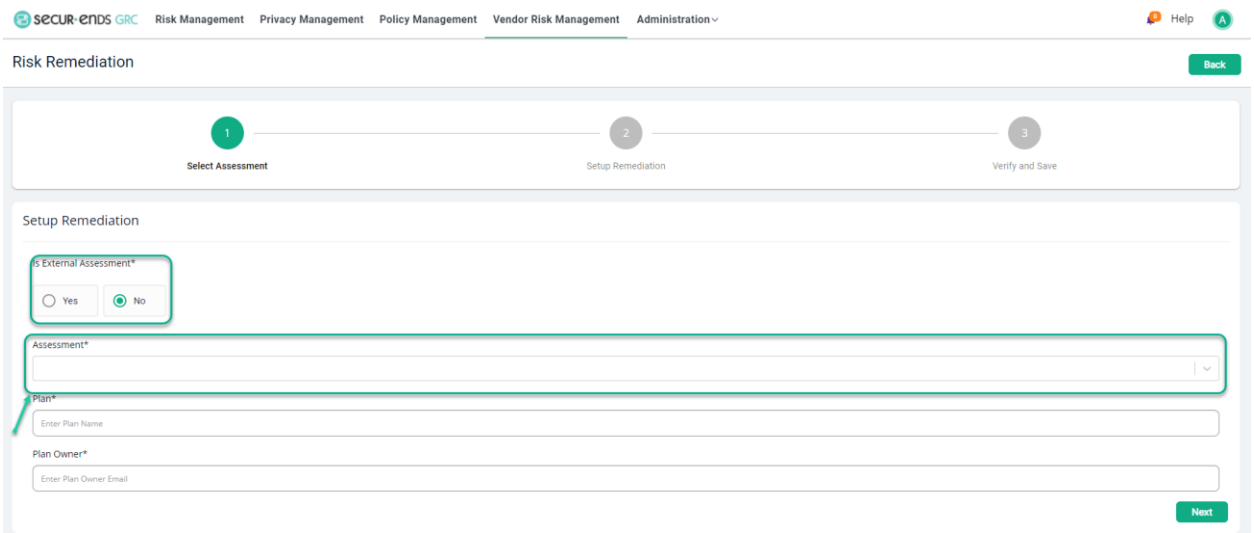


Click the Add button to follow three step process.

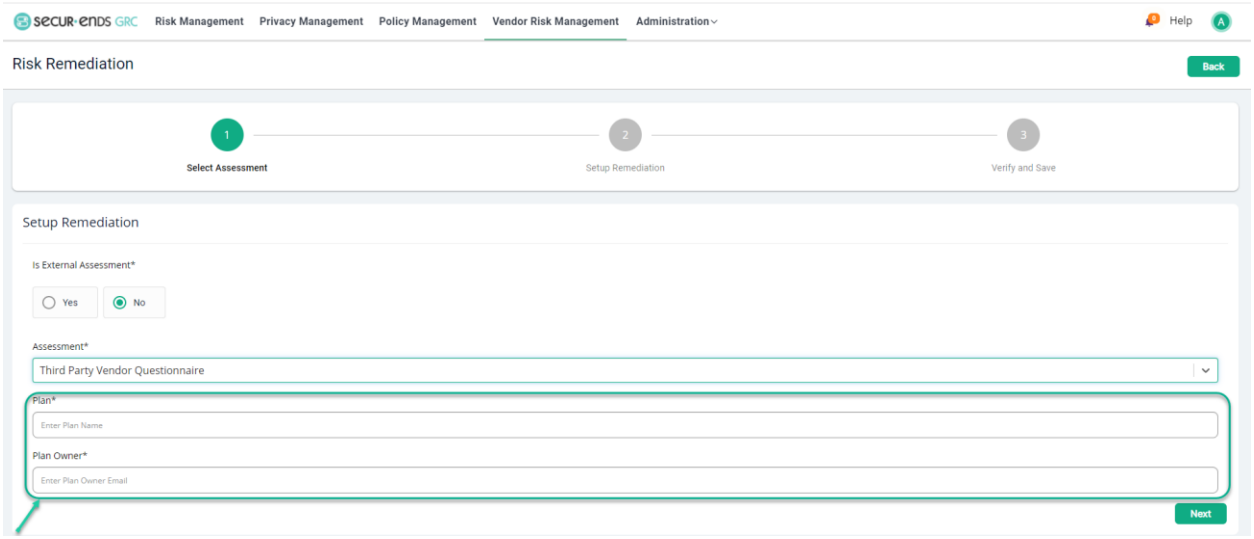


1.3.1 Step 1: Select Assessment

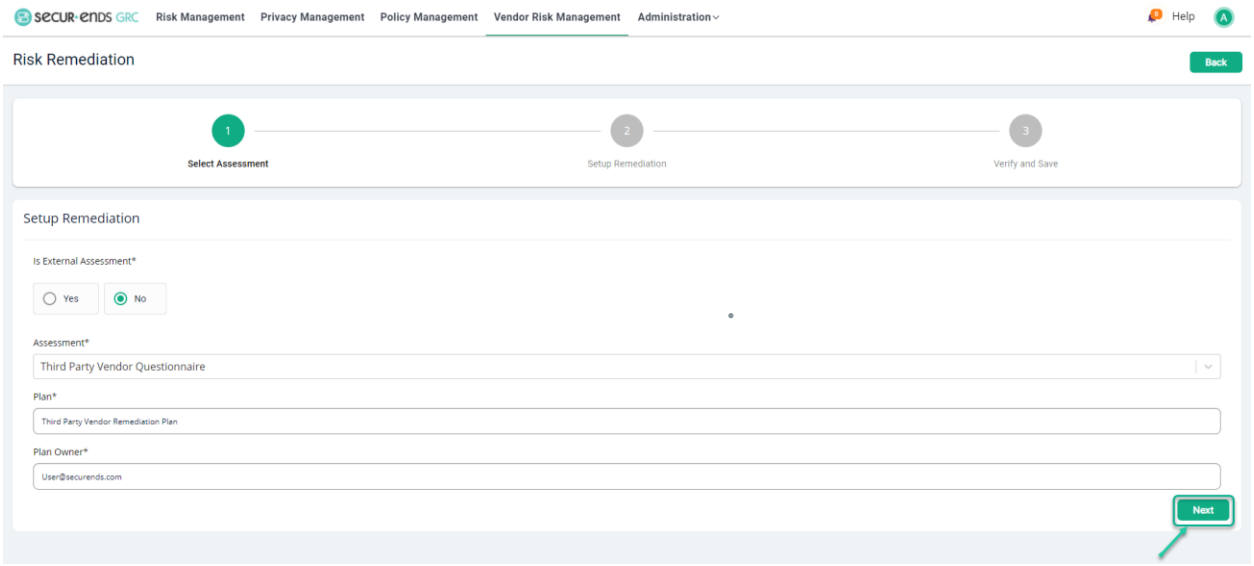
Select **External Assessment** option and **Assessment** from the drop-down list.



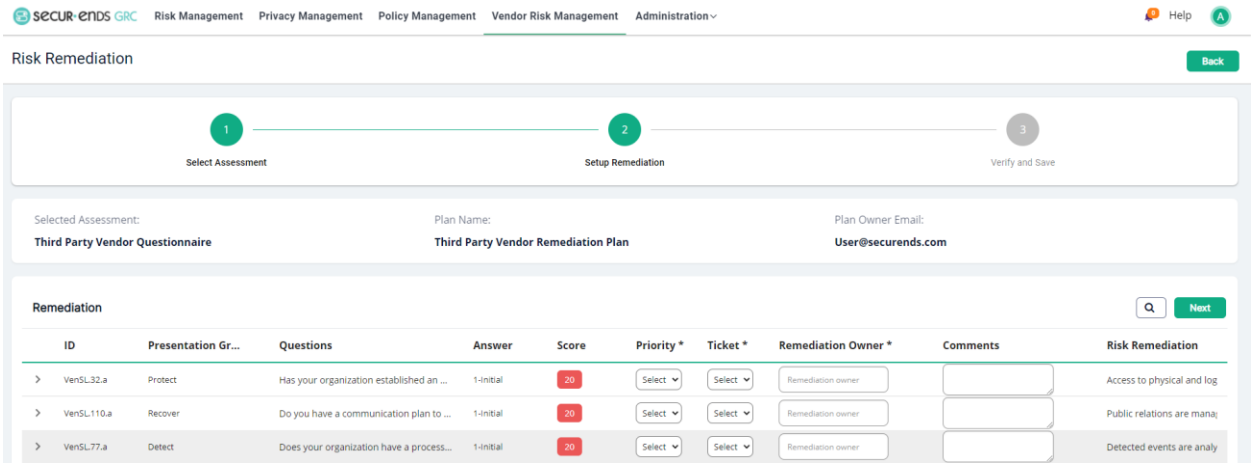
Enter a **Plan name** and **Plan Owner.**



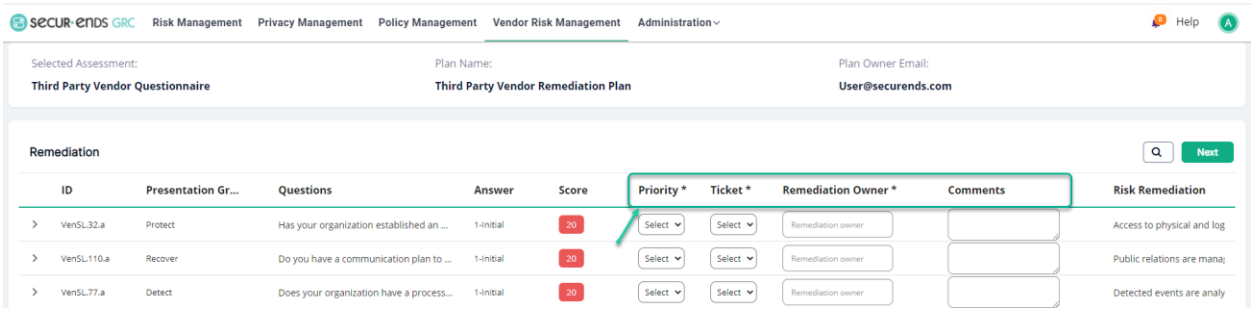
Click the **Next** button.



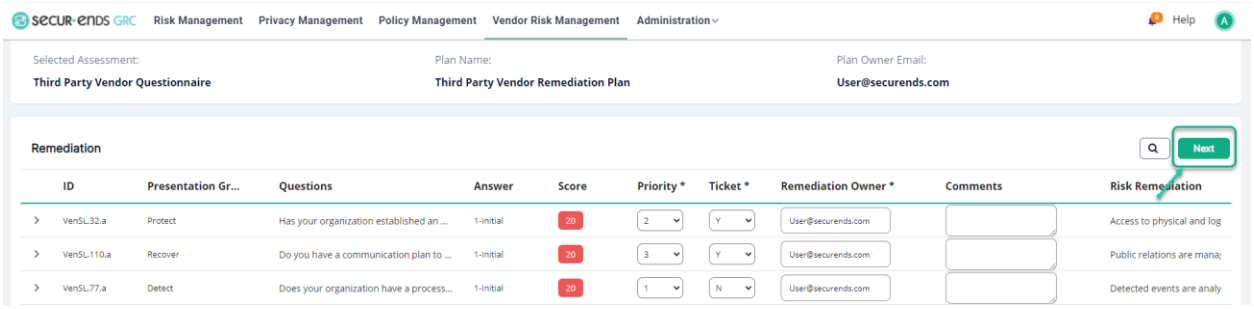
1.3.2 Step 2: Setup Remediation



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.

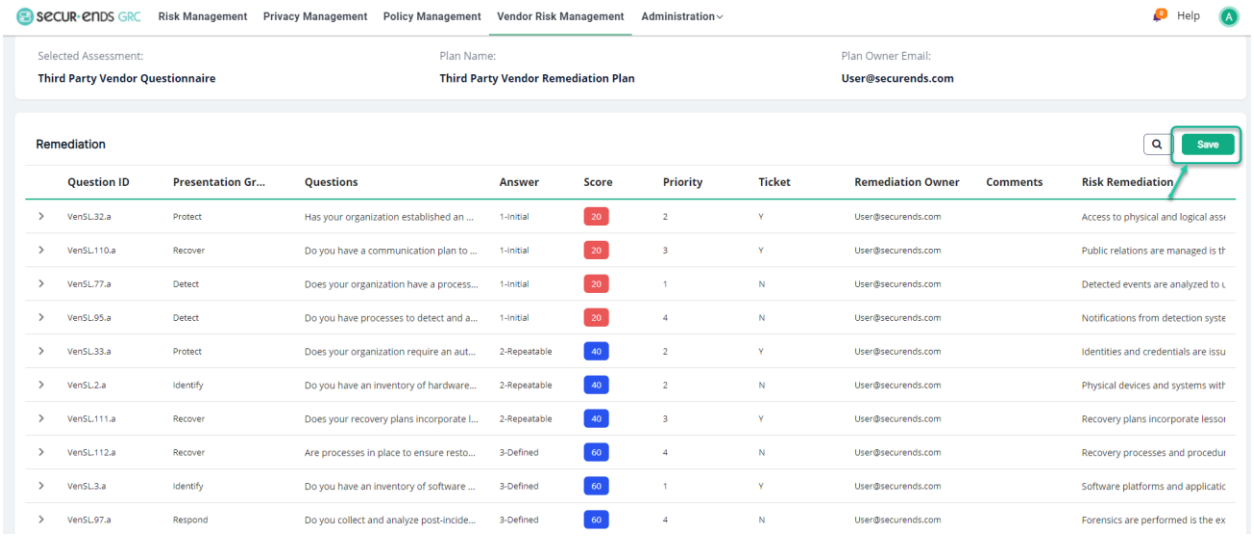


Click the **Next** button.

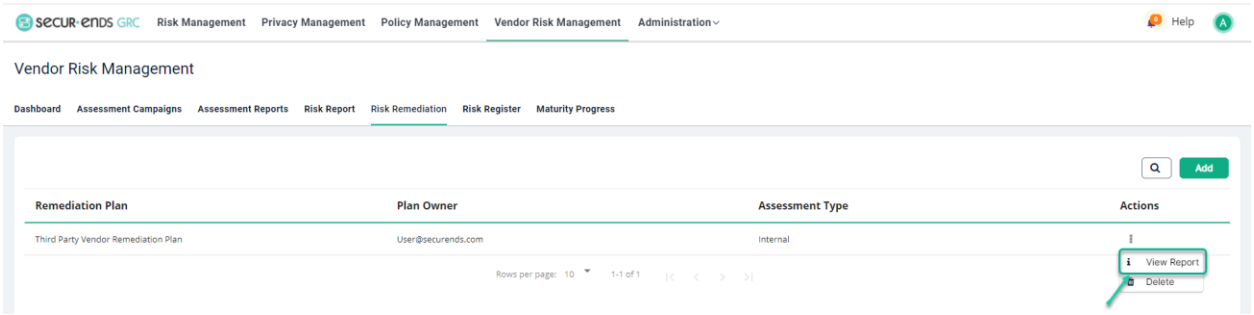


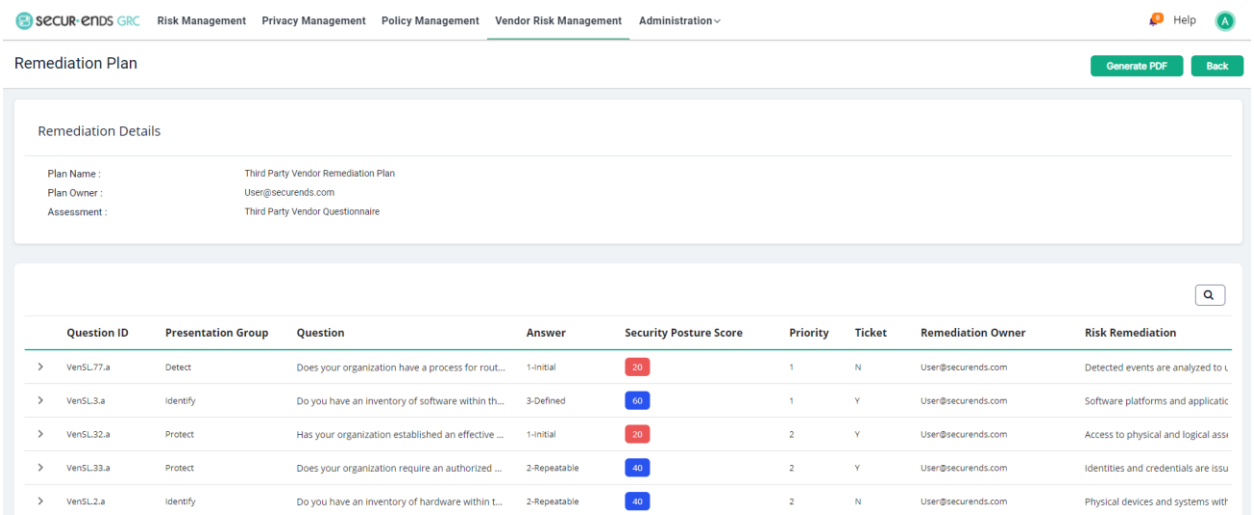
1.3.3 Step 3: Verify and Save

Click the **Save** button.



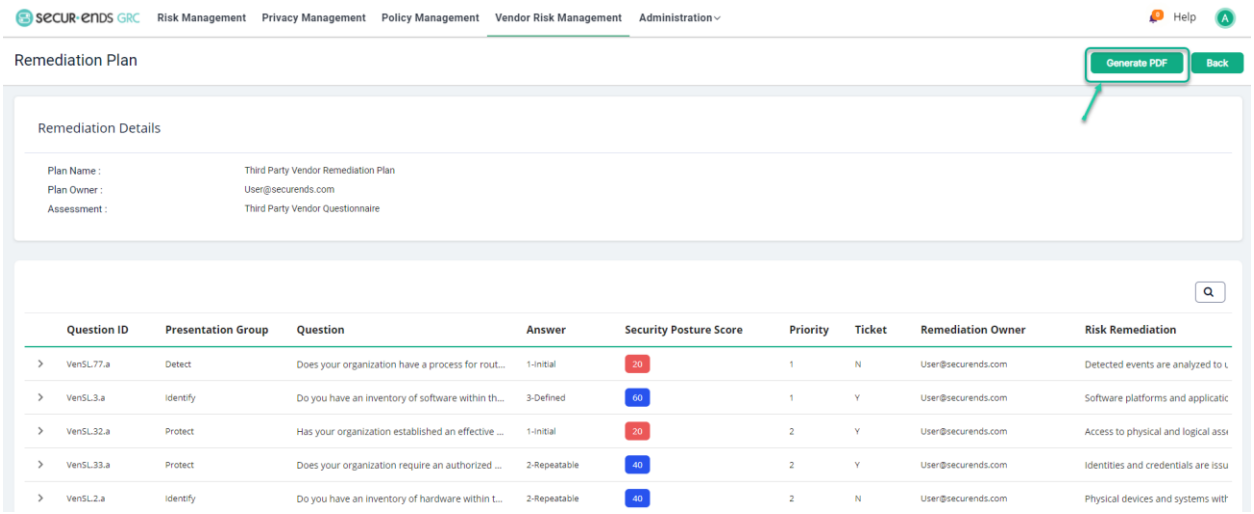
Click the **Actions Menu** and select **View Report** option.



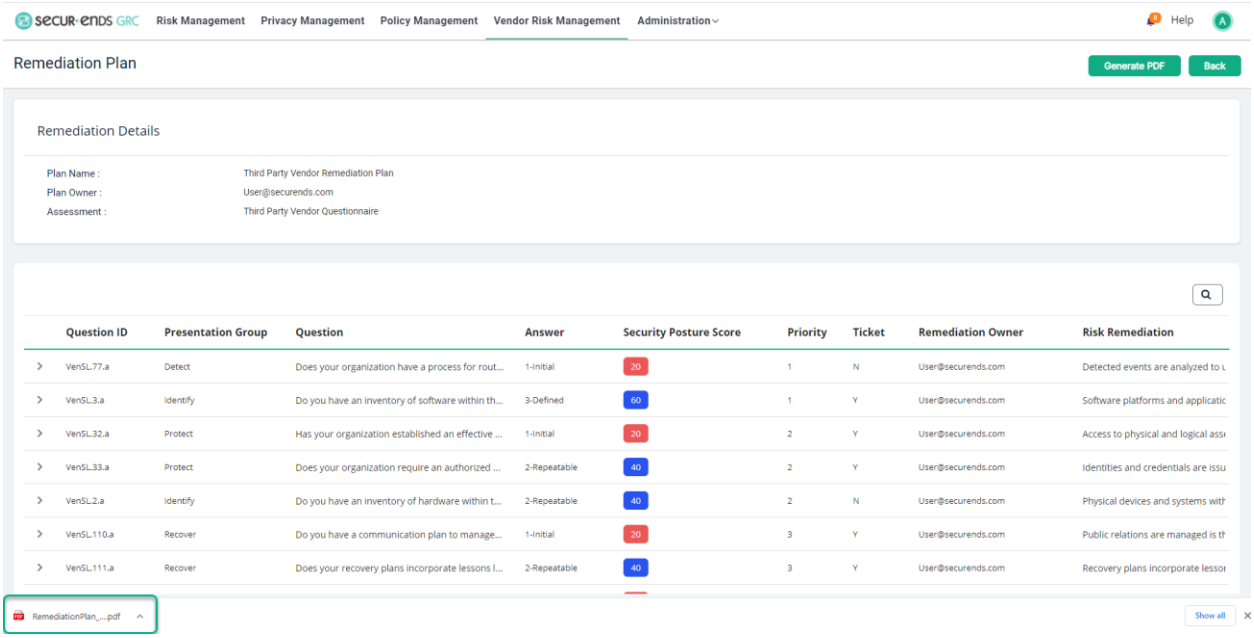


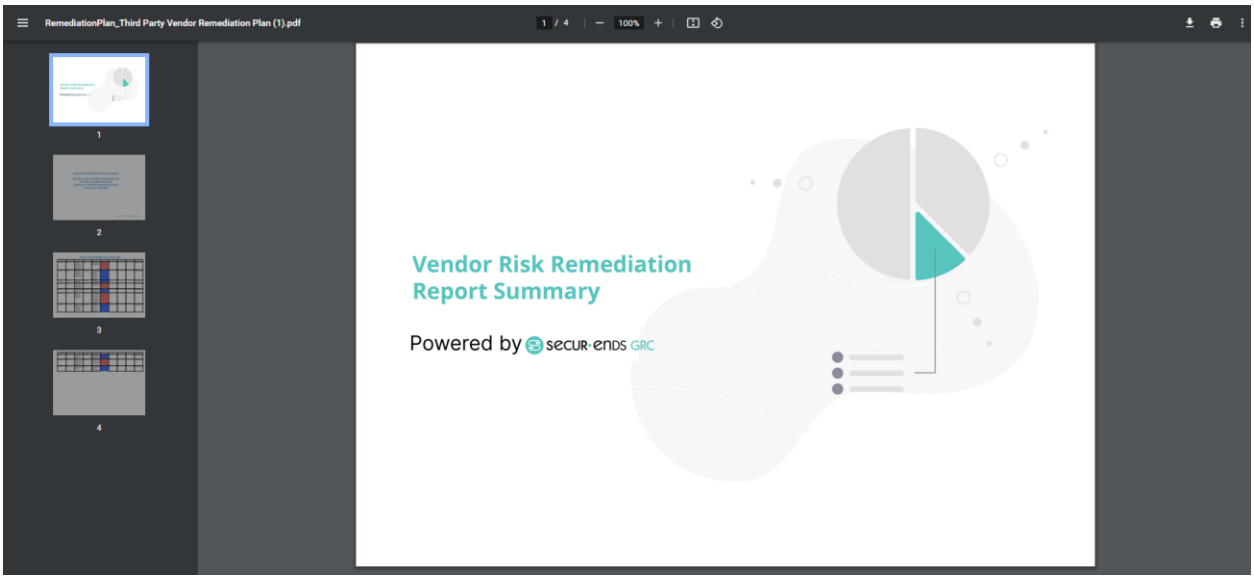
Generate Remediation Plan Report

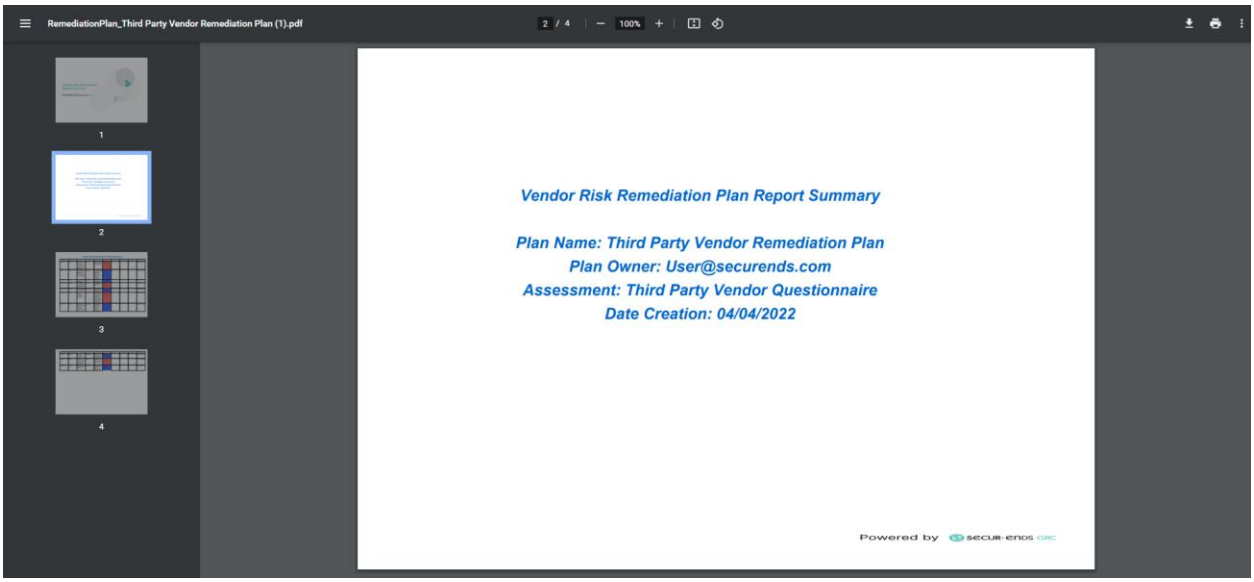
Click the **Generate PDF** button.

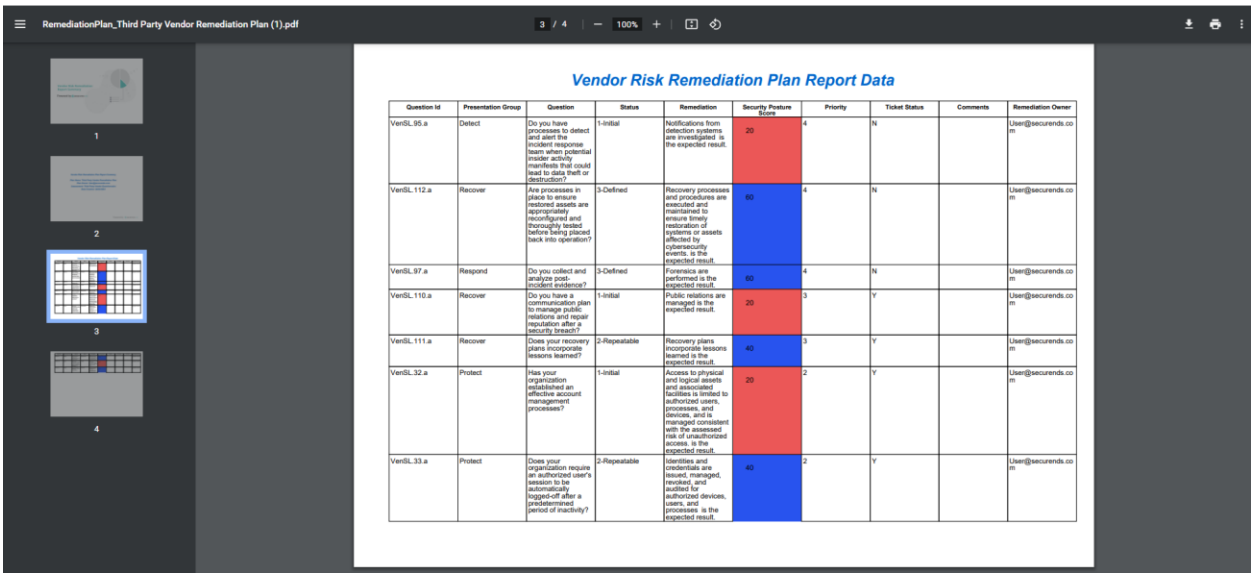


Open or Save the PDF.





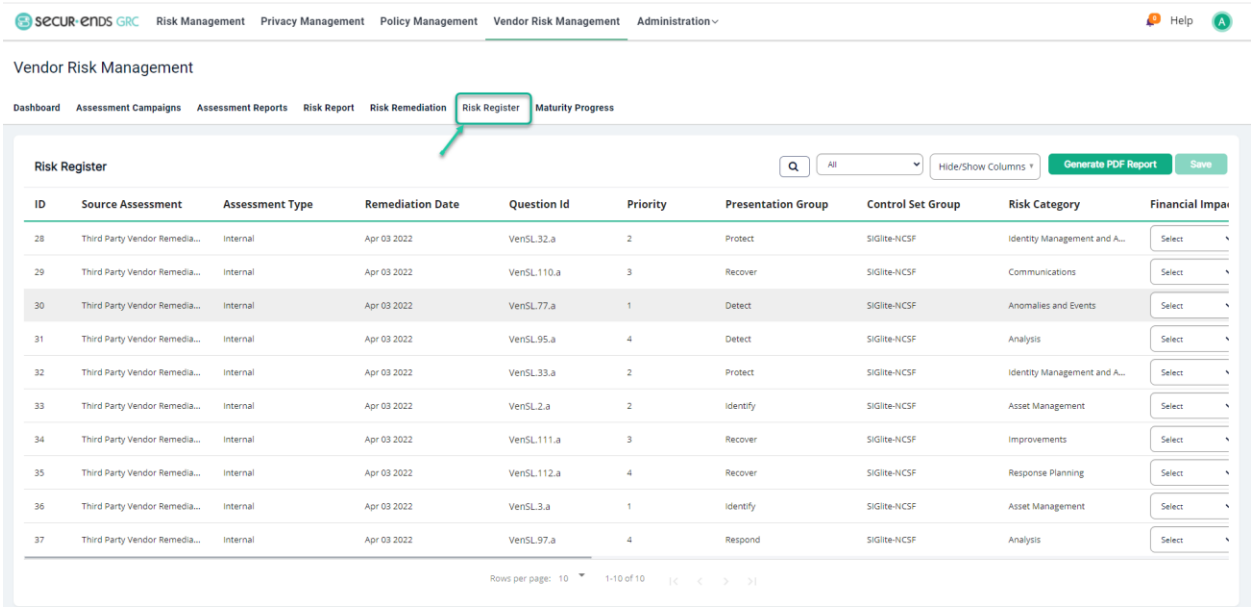




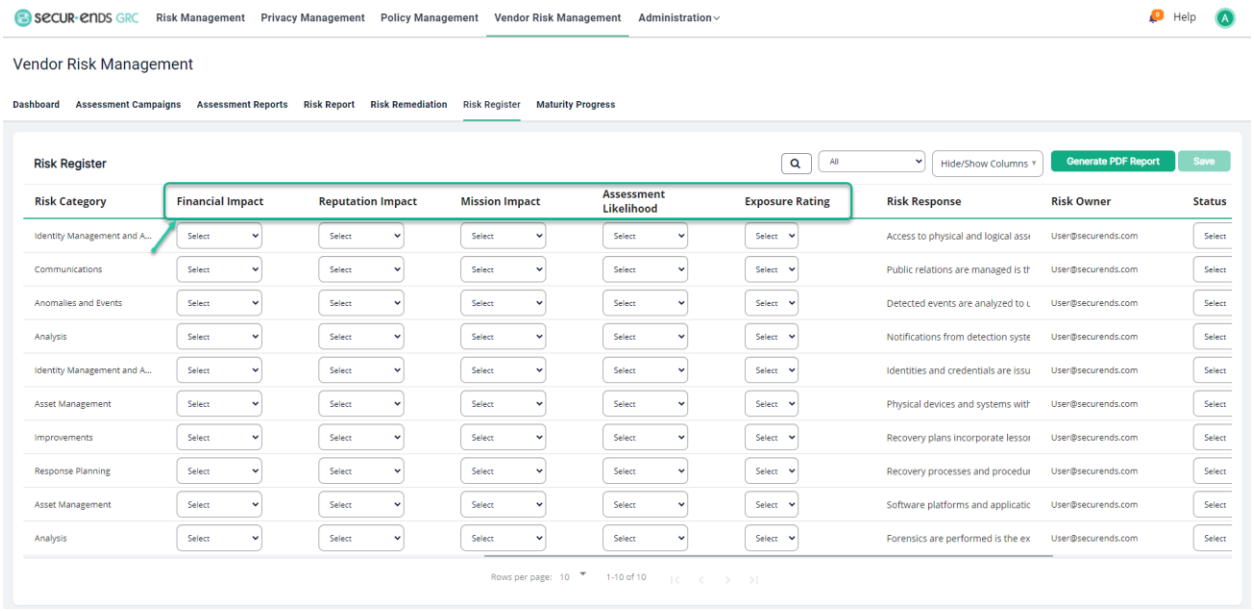
Question Id	Presentation Group	Question	Status	Remediation	Security Posture Score	Priority	Ticket Status	Comments	Remediation Owner
VenSL.95.a	Detect	Do you have processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction?	1-Initial	Notifications from detection systems are investigated is the expected result.	20	4	N		User@securends.com
VenSL.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. is the expected result.	60	4	N		User@securends.com
VenSL.97.a	Respond	Do you collect and analyze post-incident evidence?	3-Defined	Forensics are performed is the expected result.	60	4	N		User@securends.com
VenSL.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 is the expected result.	20	3	Y		User@securends.com
VenSL.111.a	Recover	Does your recovery plans incorporate lessons learned?	2-Repeatable	Recovery plans incorporate lessons learned is the expected result.	40	3	Y		User@securends.com
VenSL.32.a	Protect	Has your organization established an effective account management processes?	1-Initial	Access to physical and logical assets and 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.	20	2	Y		User@securends.com
VenSL.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	Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes is the expected result.	40	2	Y		User@securends.com

1.4 Risk Register

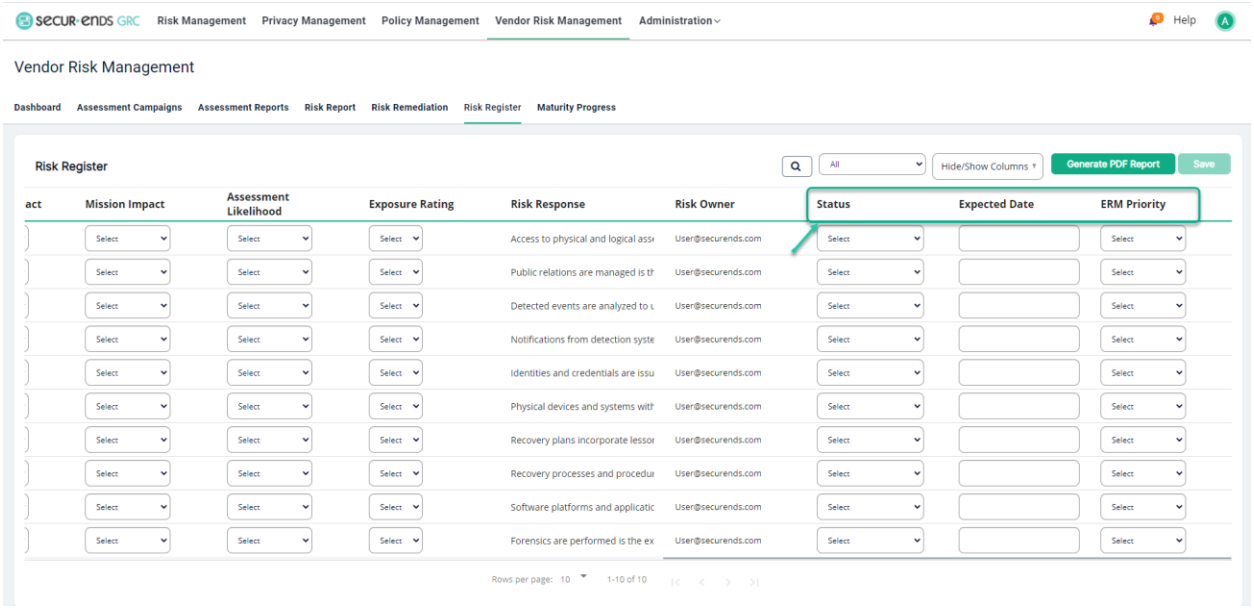
Click the **Vendor Risk Management** tab on the main menu and select **Risk Remediation** tab.



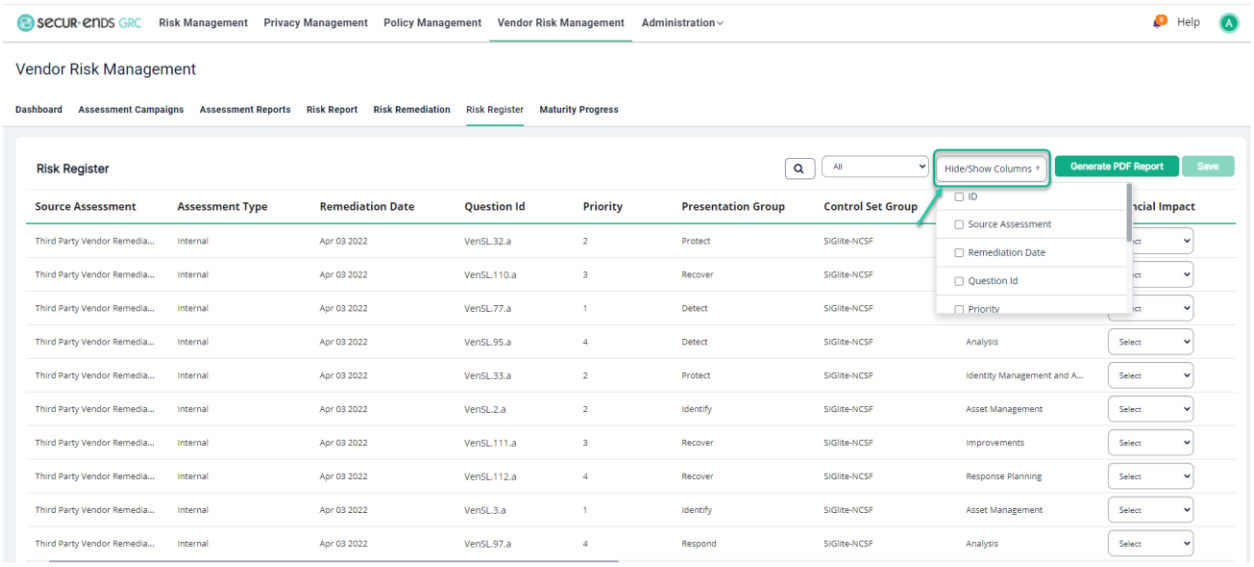
Select **Financial Impact**, **Reputation Impact**, **Mission Impact**, **Assessment Likelihood**, **Exposure Rating** drop-down menus.

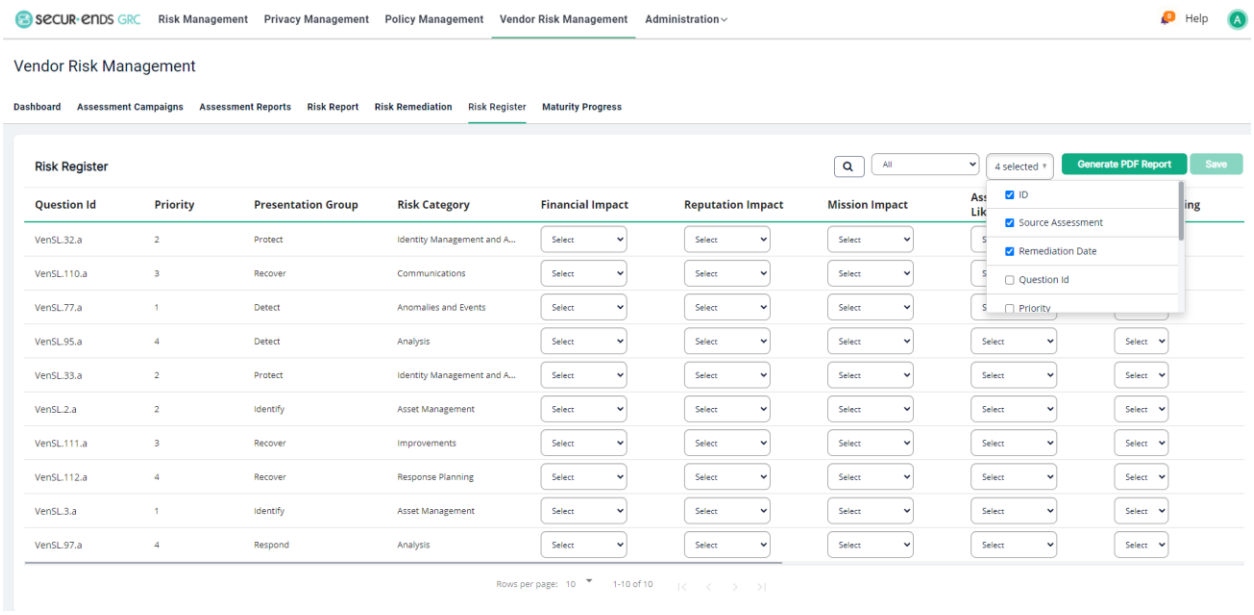


Select **Status**, **ERM Priority** in drop-down menus and enter **Expected Date.**

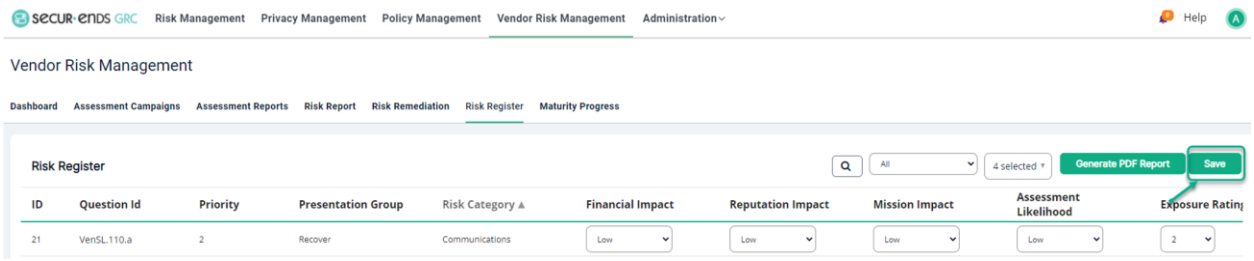


Select **Hide/Show Columns** in the drop-down menu.



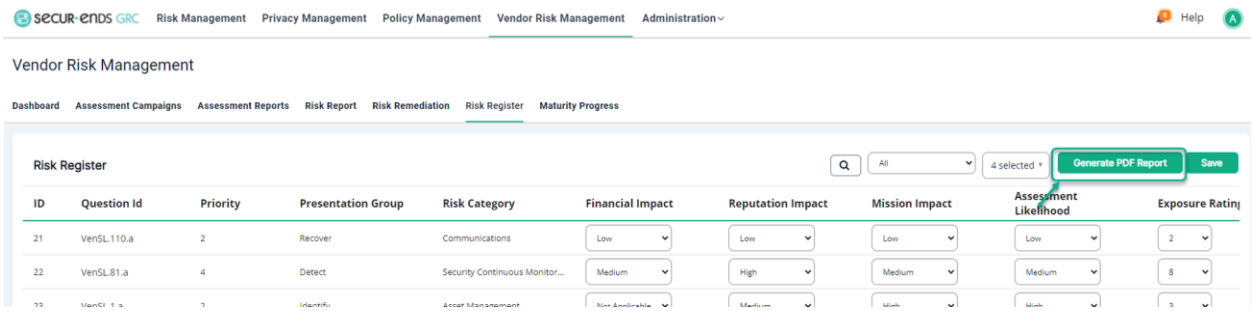


Click the **Save** button.

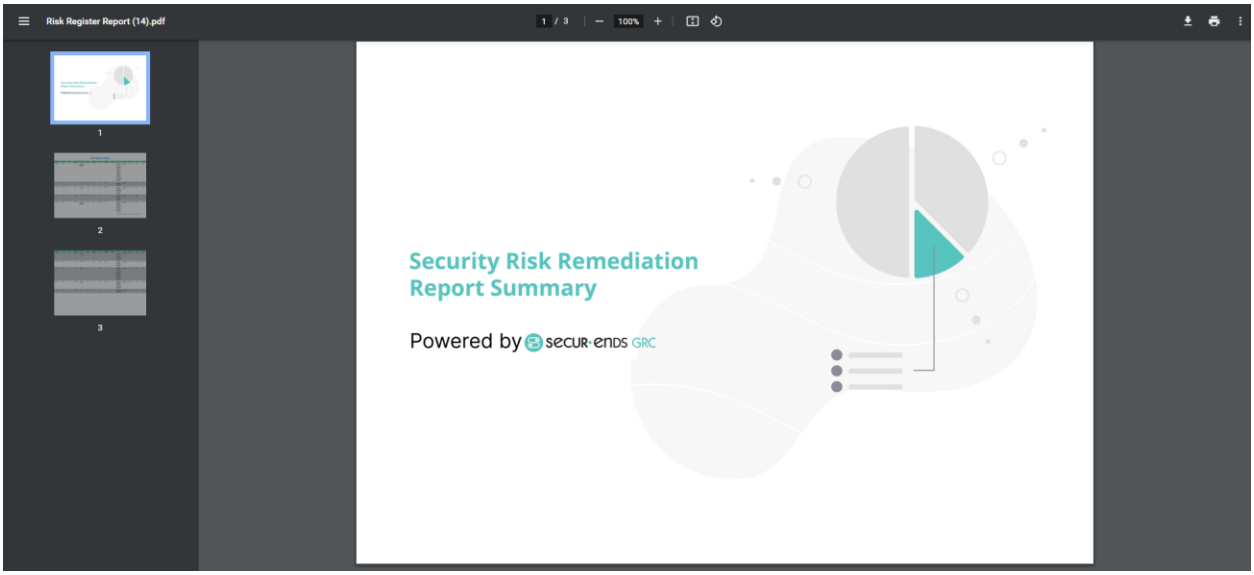


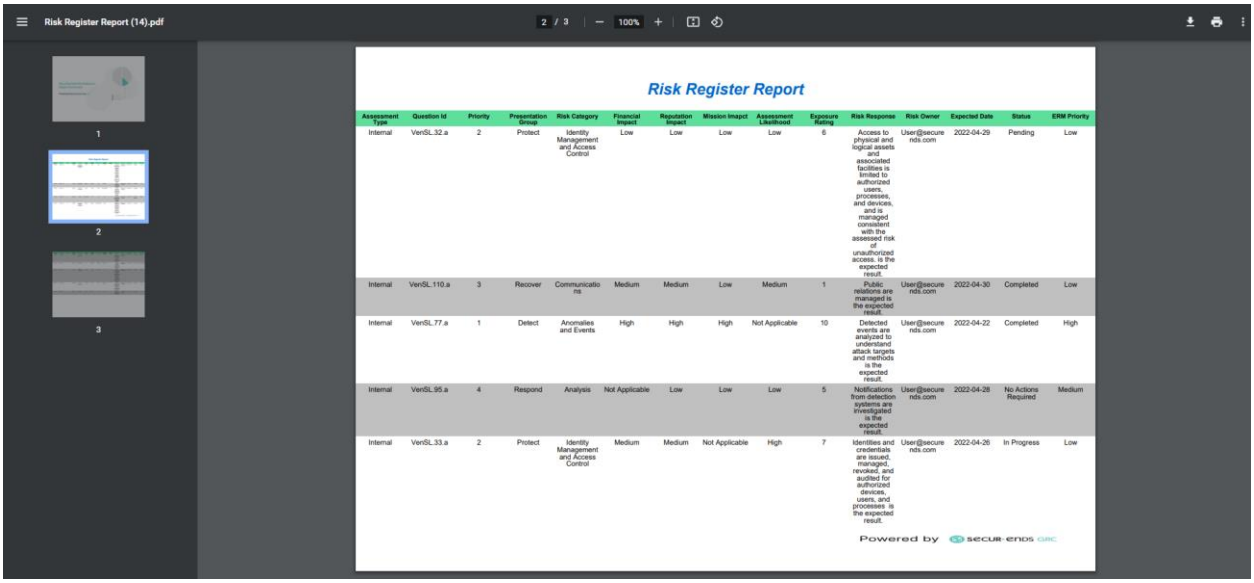
Generate Remediation Plan Report

Click the **Generate PDF Report** button.



Open or Save PDF Report as available through the browser.

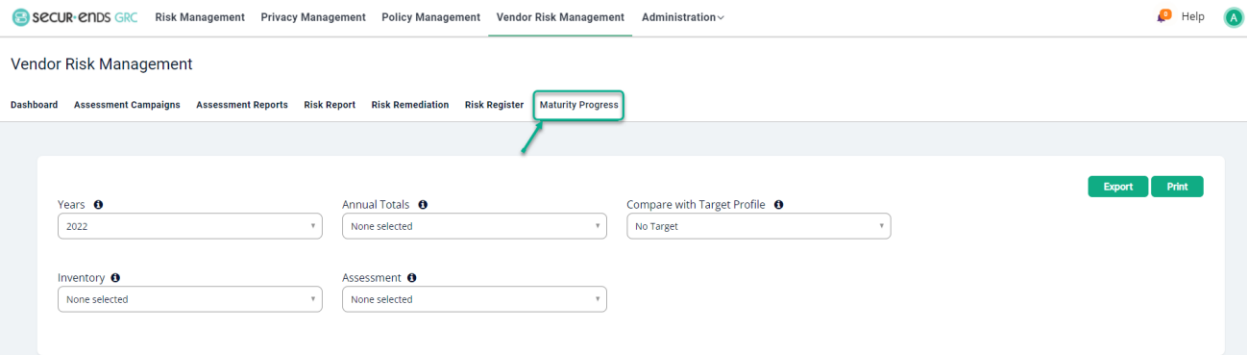




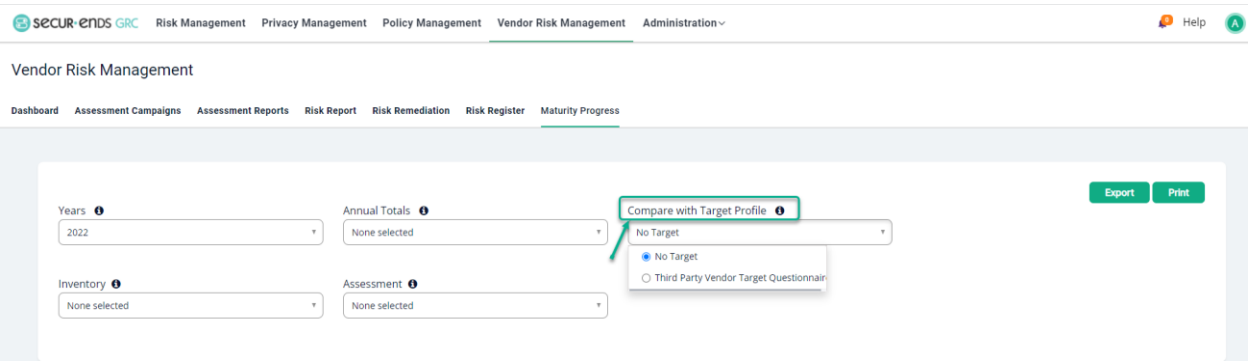
Assessment Type	Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Expected Date	Status	ERM Priority
Internal	VenSL.32.a	2	Protect	Identity Management and Access Control	Low	Low	Low	Low	6	Access to physical and logical assets and 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@securends.com	2022-04-29	Pending	Low
Internal	VenSL.110.a	3	Recover	Communications	Medium	Medium	Low	Medium	1	Public relations are managed is the expected result.	User@securends.com	2022-04-30	Completed	Low
Internal	VenSL.77.a	1	Detect	Anomalies and Events	High	High	High	Not Applicable	10	Detected events are analyzed to understand attack targets and methods is the expected result.	User@securends.com	2022-04-22	Completed	High
Internal	VenSL.95.a	4	Respond	Analysis	Not Applicable	Low	Low	Low	5	Notifications from detection systems are investigated is the expected result.	User@securends.com	2022-04-28	No Actions Required	Medium
Internal	VenSL.33.a	2	Protect	Identity Management and Access Control	Medium	Medium	Not Applicable	High	7	Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes is the expected result.	User@securends.com	2022-04-26	In Progress	Low

1.5 Maturity Progress

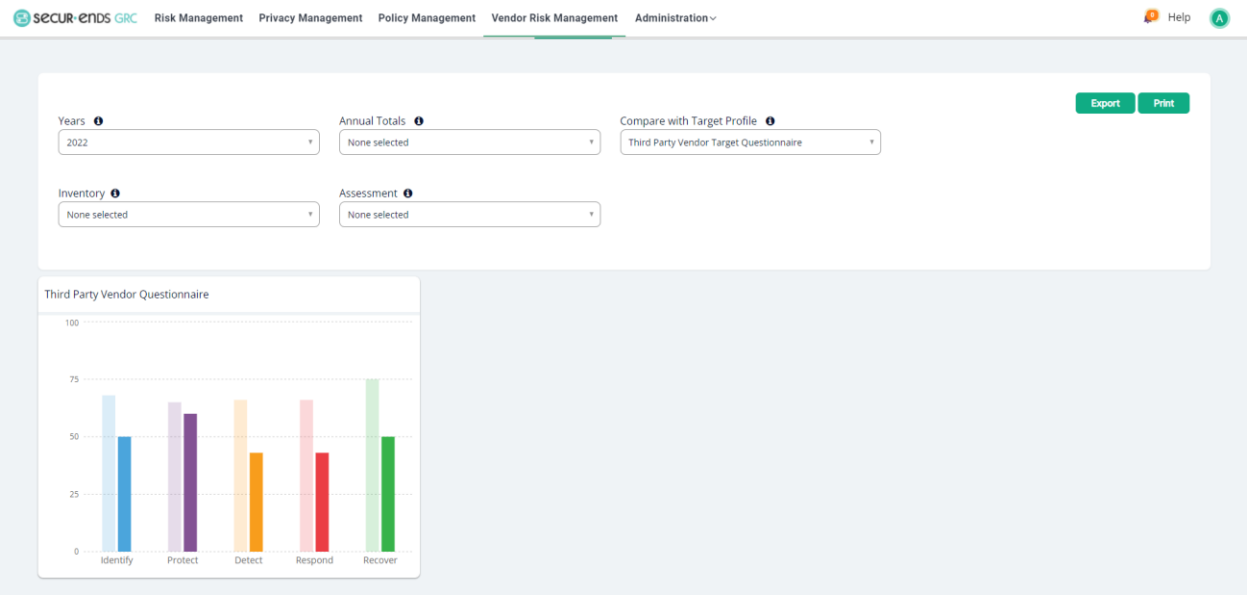
Click the **Vendor Risk Management** tab on the main menu and select **Maturity Progress** tab.



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]