



Risk Management User Guide



Table of Contents

Overview.....	2
1 Risk Management.....	3
1.1 Dashboard.....	3
1.2 Assessment Campaigns.....	4
1.2.1 Step 1: Select or Create Assessment Template.....	4
1.2.2 Step 2: Schedule Details.....	8
1.2.3 Step 3: Verify and Launch.....	11
1.3 Assessment Reports.....	16
1.4 Risk Report.....	17
1.5 Risk Remediation.....	20
1.5.1 Step 1: Select Assessment.....	20
1.5.2 Step 2: Setup Remediation.....	22
1.5.3 Step 3: Verify and Save.....	23
1.6 Risk Register.....	26
1.7 Maturity Progress.....	30

Overview

This Risk Management 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 Risk Management User Guide will enable the administrator to tailor complex campaigns for each organization.

What we do!

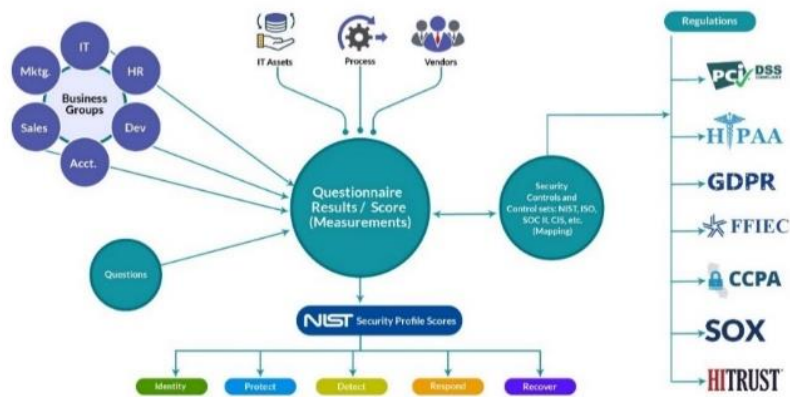
Securends GRC is an accessible SaaS solution that helps achieve a reliable enterprise security score through a simple interface. It can be managed quarterly or annually, even by those who lack experience with managing security or compliance controls. The Securends GRC method of completing risk assessments 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 measured responses or utilize the capability to reassign 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 Risk Management User Guide 1.0	1.0	April 7, 2022

1 Risk Management



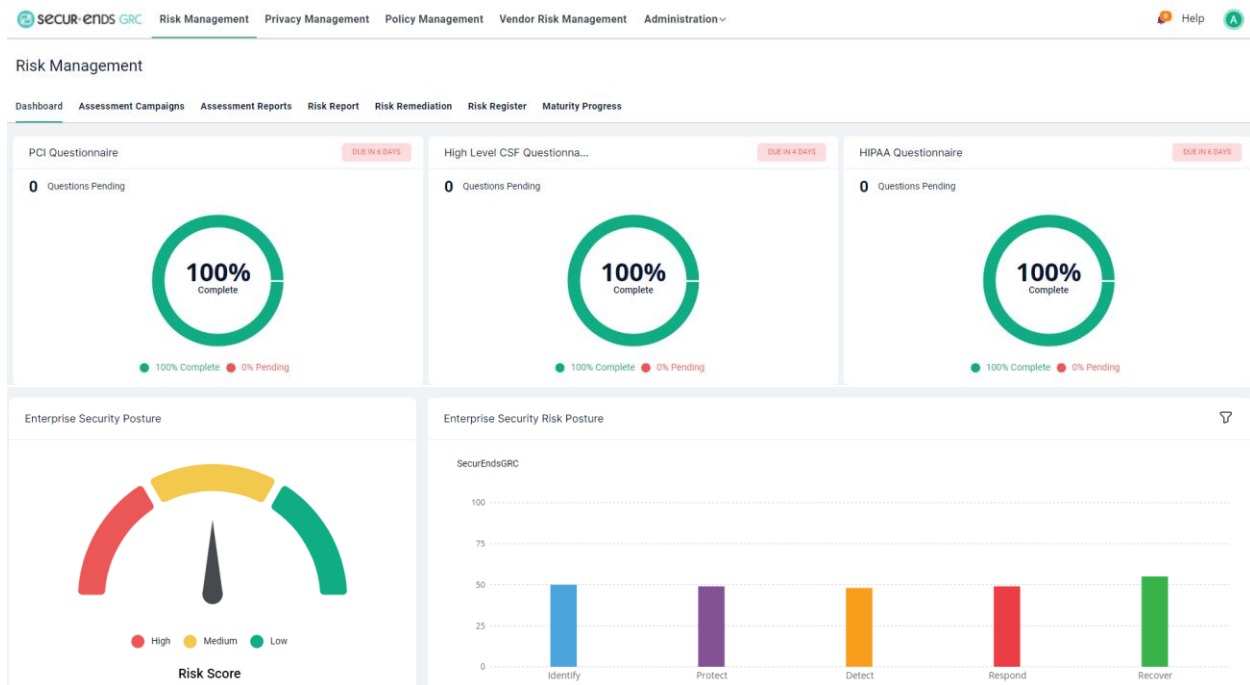
Out of the box features enable organizations to integrate accountability and process governance which will enhance the speed and efficiency risk management as delivered across all compliance frameworks.

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

Note: For Risk Management setup of Assets/Process/Entities under Inventory refer to the *Administration User Guide* document).

1.1 Dashboard

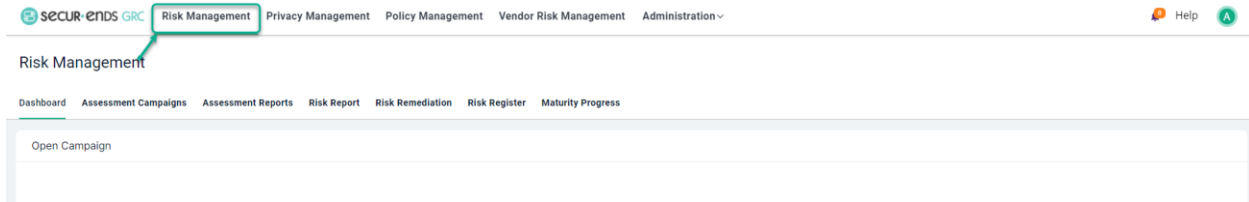
View the last three assessment campaigns that were launched and see the high-level scoring of all the assessments in the charts. Use the filter option to narrow the scoring perspective to a specific level of the business hierarchy.



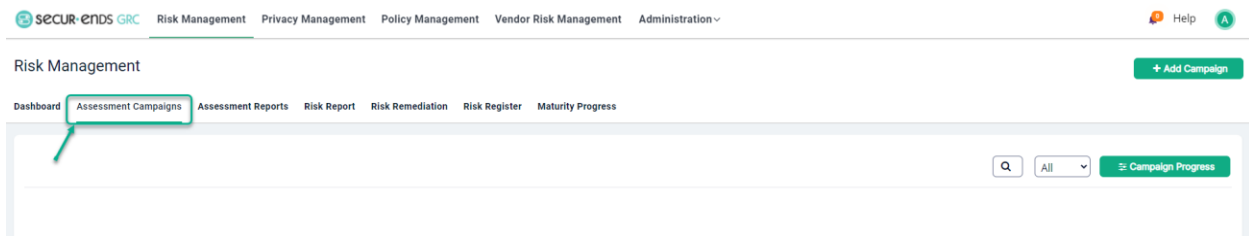
1.2 Assessment Campaigns

Configuration of the assessment campaigns is a simple process found under the “Assessment Campaigns” menu option. It is the first activity along the risk management life cycle menu options.

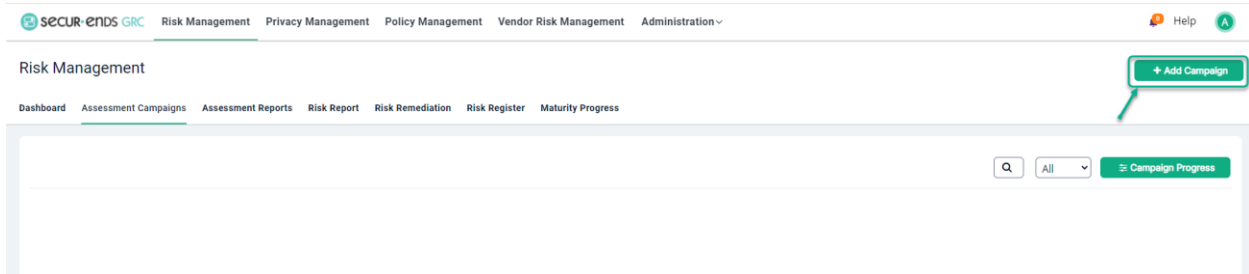
Select the **Risk Management** tab on the main menu.



Select **Assessment Campaigns** Tab.

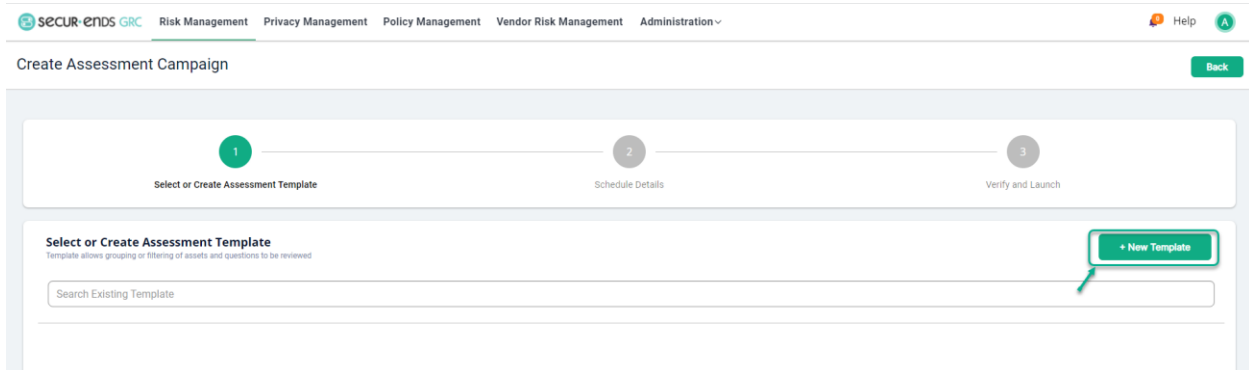


Click the **Add Campaign** button on the top right corner to follow the three-step process.



1.2.1 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* [Text Field]
Description* [Text Field]
Inventory Type* Assets Process Entities Connectors

Close Save

Click the **Assets** radio button and select the asset from the dropdown list (these options were previously configured in the Administration, Inventory menu).

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* High Level Cyber Security Assessments(NIST CSF)
Description* High level Cyber Security System
Inventory Type* Assets Process Entities Connectors
Assets High Level Cyber Security Assessments(NIST CSF) [Dropdown]
[Search Bar]
[Select all]
[CSF Target Assessment]
[High Level Cyber Security Assessments(NIST CSF)] [No]

Actions View Questionnaire

Close Save

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

or

Click the **No** radio button (to select a list of filtered questions) and then click the **Select/Unselect Questionnaire** button.

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

Create Assessment Campaign

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

Template Name* High Level Cyber Security Assessments(NIST CSF)

Description* High level Cyber Security System

Inventory Type* Assets Process Entities Connectors

Assets High Level Cyber Security Assessments(NIST CSF)

Assets	Include All Questions	Actions
High Level Cyber Security Assessments(NIST CSF)	<input type="radio"/> Yes <input checked="" type="radio"/> No	Select/Unselect Questionnaire

Close Save

Click the **Apply Filter** symbol.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management High Level Cyber Security Assessments(NIST CSF)

1 Select or Create Assessment Template

Template Name* High Level Cyber Security Assessments(NIST CSF)

Description* High level Cyber Security System

Inventory Type* Assets Process Entities Connectors

Assets High Level Cyber Security Assessments(NIST CSF)

Apply Filter

- Select All Questions in the page
- HL.ID.1: Are the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes identified and managed consistent with their relative importance to business objectives and the organization's risk strategy?
- CSF.ID.AM-1: Are physical devices and systems within the organization inventoried?
- CSF.ID.AM-2: Are software platforms and applications within the organization inventoried?
- CSF.ID.AM-3: Are organizational communication and data flows mapped?
- CSF.ID.AM-4: Are the external information systems catalogued?
- CSF.ID.AM-5: Are resources (e.g. hardware, Devices, Data, Time, and software) prioritized based on their classification, criticality, and business value?
- CSF.ID.AM-6: Are the cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) established?
- HL.ID.2: Are the organization's mission, objectives, stakeholders, and activities understood and prioritized, and used to inform cybersecurity roles, responsibilities, and risk management decisions?

Choose Filter **Question ID**, **Question** or **Policy** or **Role**.

Filter Questionnaire

Choose filter

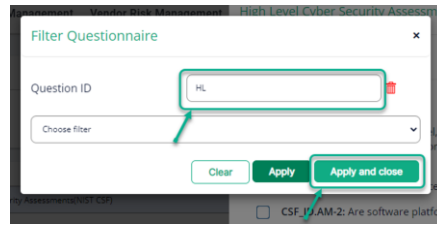
Clear Apply Apply and close

Filter Questionnaire

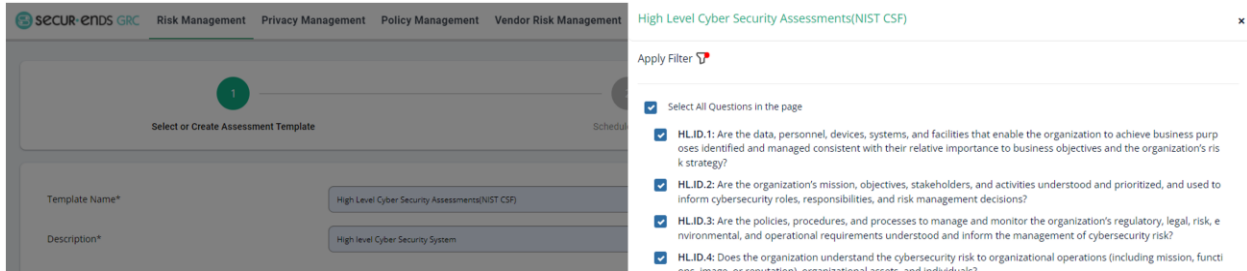
Choose filter

- Choose filter
- Question ID
- Question or Policy
- Role

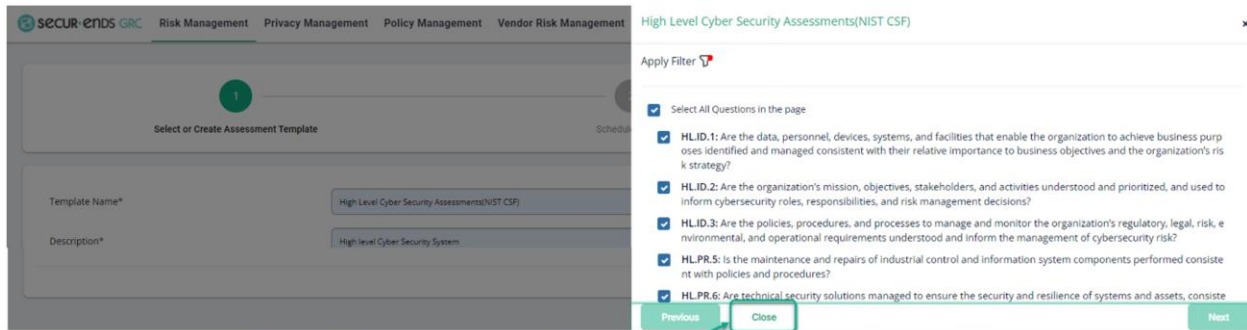
Enter a portion of the **Question ID** and then click on **Apply and Close** button.



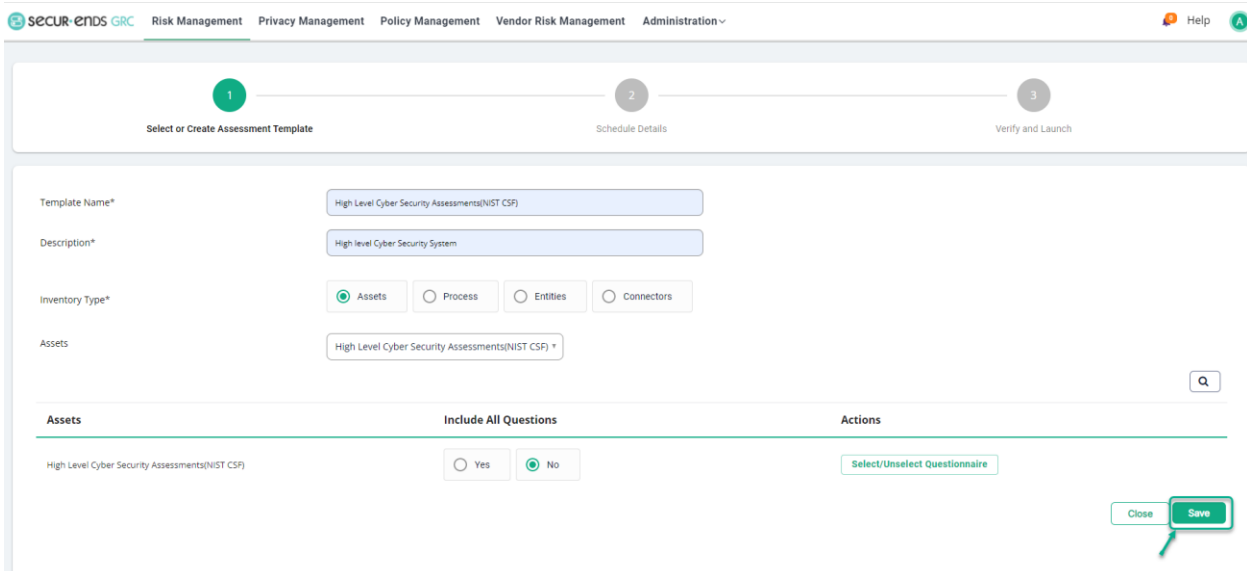
Check the box for **Select All Questions in the page**.



Click the **Close** button.



Click the **Save** button.



Select the Assessment **Template** that was created.

The screenshot shows the 'Create Assessment Campaign' page with a progress bar at the top indicating three steps: 1. Select or Create Assessment Template (active), 2. Schedule Details, and 3. Verify and Launch. Below the progress bar, the page title is 'Select or Create Assessment Template'. A search bar for existing templates is present. A list of templates is shown, with 'High Level Cyber Security Assessments(NIST CSF)' selected. A callout box highlights the 'Select Template' button.

1.2.2 Step 2: Schedule Details Assessment Configuration

Enter a unique **Assessment Campaign Name**.

(Including a descriptive title is helpful for later management of the assessment. I.e., include the quarter and year in the title as “Q1 2022” as is helpful for identifying and comparing assessments).

The screenshot shows the 'Create Assessment Campaign' page with the progress bar now highlighting Step 2: Schedule Details. The page title is 'Assessment Configuration'. The selected template is 'High Level Cyber Security Assessments(NIST CSF)'. A callout box highlights the 'Assessment Campaign Name' input field. Below it, there is a checkbox for 'Create a Target Campaign', 'Start Date' (04/02/2022), and 'End Date' (04/02/2022) fields. At the bottom, there are radio buttons for 'Assessment Campaign Reviewer' with options: Asset Owner (selected), Role Owner, and Alternate Reviewer.

NOTE: Target Campaign Creation

Occasionally a Target Campaign should be created to compare the future state to the current assessments. To create a Target Campaign, select the **Create a Target Campaign** option and enter an **Alternate Reviewer**. This person should understand the assessment requirements enough to set the goals for the future state.

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

Assessment Configuration

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM a day ago

Assessment Campaign Name
NIST CSF Target Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/02/2022

Assessment Campaign Reviewer

Alternate Reviewer

Search Reviewer Clear OR

Final Approver

Campaign Reminders

Send reminder email to reviewer

Campaign Instructions
Default

Select a **Start Date** and **End Date**.

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

Assessment Configuration

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM a day ago

Assessment Campaign Name
High Level CSF Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/02/2022

Assessment Campaign Reviewer

Asset Owner Role Owner Alternate Reviewer

Select **Asset Owner**, **Role owner**, or **Alternate Reviewer**.

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

Assessment Configuration

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM a day ago

Assessment Campaign Name
High Level CSF Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/30/2022

Assessment Campaign Reviewer

Asset Owner Role Owner Alternate Reviewer

Final Approver

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

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

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM a day ago

Assessment Campaign Name
High Level CSF Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/30/2022

Assessment Campaign Reviewer

Asset Owner Role Owner Alternate Reviewer

Final Approver
Search [Clear]

Campaign Reminders

Send reminder email to reviewer

Select **Campaign Reminders** option. (By selecting this option, the reminder email can send to Reviewer).

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

Assessment Configuration

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM a day ago

Assessment Campaign Name
High Level CSF Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/30/2022

Assessment Campaign Reviewer

Asset Owner Role Owner Alternate Reviewer

Final Approver

Campaign Reminders
 Send reminder email to reviewer

Campaign Instructions
Default

Back Next

Click the **Next** button.

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

Assessment Configuration

High Level Cyber Security Assessments(NIST CSF)
April 1, 2022 11:49 AM + 6hr ago

Assessment Campaign Name
High Level CSF Questionnaire

Create a Target Campaign

Start Date: 04/02/2022 End Date: 04/30/2022

Assessment Campaign Reviewer
 Asset Owner Role Owner Alternate Reviewer

Final Approver

Campaign Reminders
 Send reminder email to reviewer

Campaign Instructions
Default

Back Next

1.2.3 Step 3: Verify and Launch

Click the **Preview** button.

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

Launch Campaign

High Level CSF Questionnaire Ready

04/02/2022 Campaign Start Date 04/30/2022 Campaign End Date

User@securends.com Reviewer Email ID N/A Final Approver Email ID

Preview

Click the **Launch** button.

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

Launch Campaign

High Level CSF Questionnaire Ready

04/02/2022 Campaign Start Date 04/30/2022 Campaign End Date

User@securends.com Reviewer Email ID N/A Final Approver Email ID

Launch

Questionnaire - preview

Are restoration activities coordinated with internal and external parties?

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

Is anomalous activity detected in a timely manner and the potential impact of events understood?

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

Chose to send an email notification or launch the campaign with no notification by clicking the launch button in the pop-up window. The option to exclude specific reviewers/participants is also available.

Launch Campaign

Do you want to launch this campaign?

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

Cancel **Launch**

Open the **Actions** menu and select **View** item.

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

Risk Management

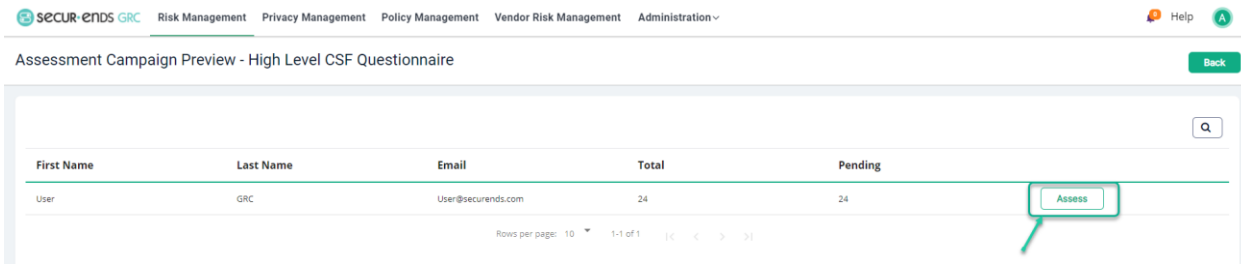
+ Add Campaign

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

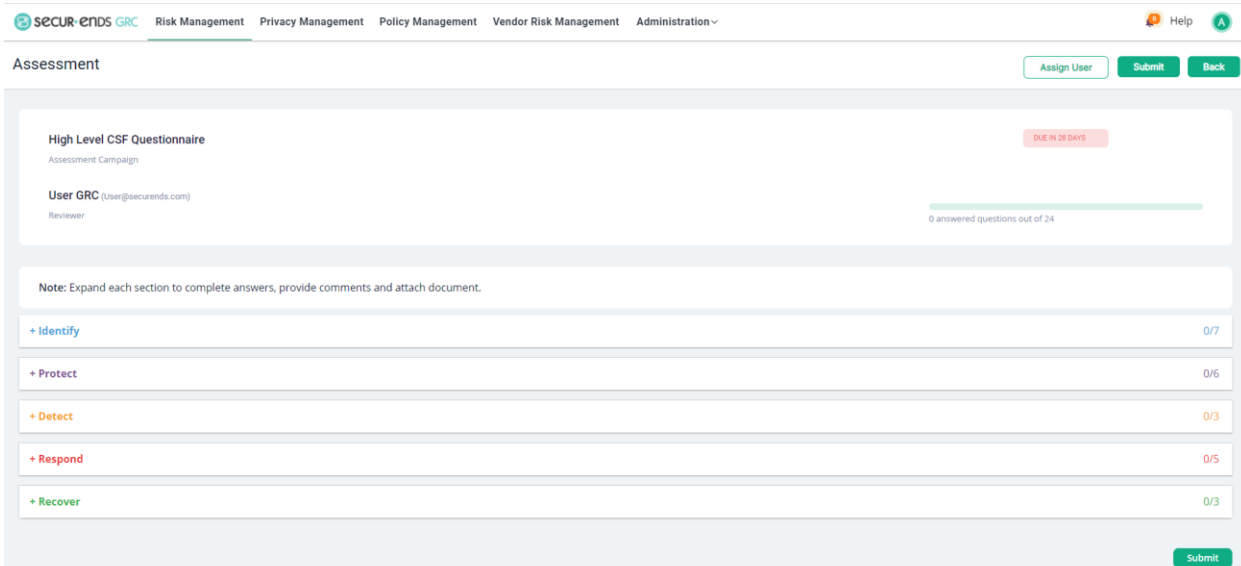
Name	Status	Start Date	End Date	Actions
High Level CSF Questionnaire	Open	Apr 02, 2022	Apr 30, 2022	<ul style="list-style-type: none">ViewDetailsEditCloseRemindDelete

Rows per page: 10 1-1 of 1

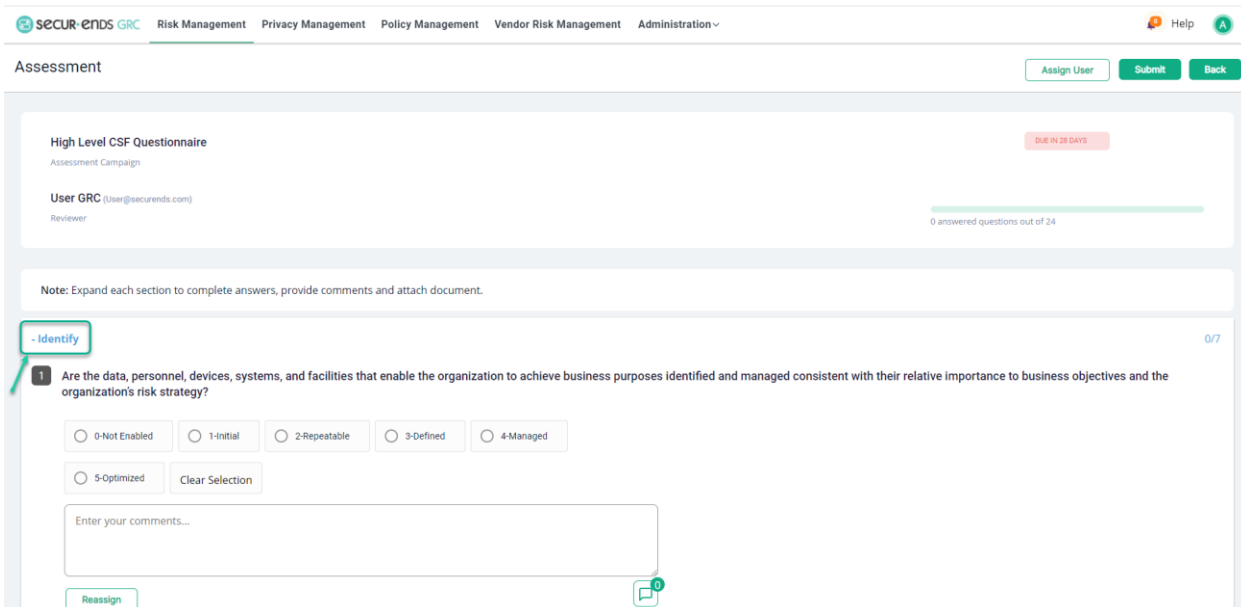
When the Reviewer participates in a campaign, they will be presented with the Assessment Campaigns page and open their assignment from the **Assess** button on the right.



The Reviewer views the campaign with the questions categorized in their security functions.



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



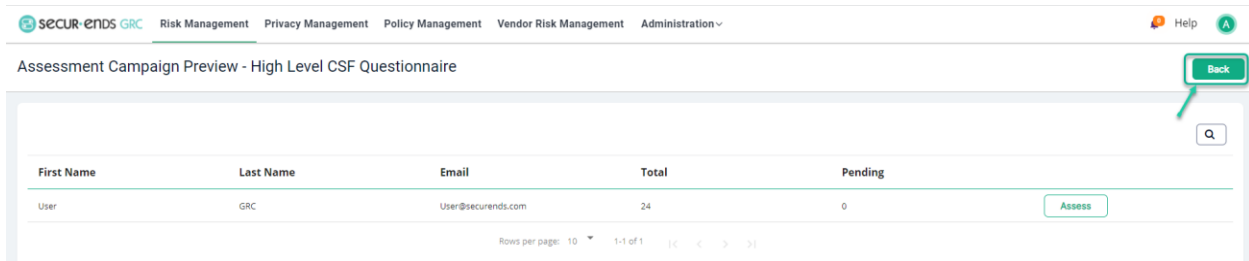
Select **Reassign** button. (Selecting this option can reassign the question to another reviewer).

The screenshot shows the SecurEnds GRC interface for a 'High Level CSF Questionnaire'. The user is 'User GRC (User@securends.com)'. A 'DUE IN 28 DAYS' badge is visible. The question is: '1 Are the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes identified and managed consistent with their relative importance to business objectives and the organization's risk strategy?'. The options are: 0-Not Enabled, 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, and 5-Optimized. A 'Clear Selection' button is present. Below the options is a text area for 'Enter your comments...'. A 'Reassign' button is highlighted with a red box and a red arrow. A 'Submit' button is also visible.

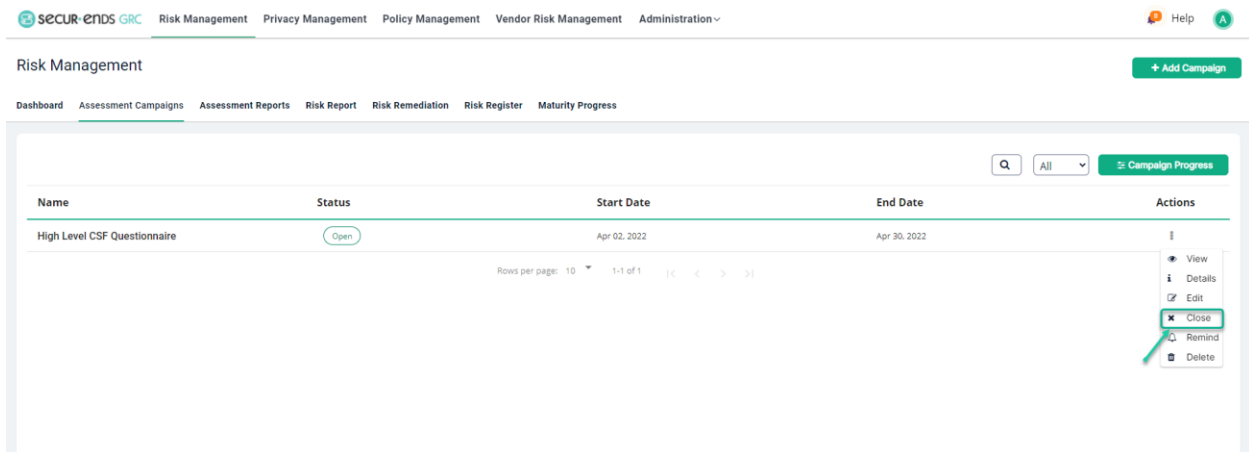
Answer all questions and click the **Submit** button.

The screenshot shows the SecurEnds GRC interface for a questionnaire question. The question is: '2 Are recovery planning and processes improved by incorporating lessons learned into future activities?'. The options are: 0-Not Enabled, 1-Initial, 2-Repeatable, 3-Defined, 4-Managed, and 5-Optimized. The '2-Repeatable' option is selected. A 'Clear Selection' button is present. Below the options is a text area for 'Enter your comments...'. A 'Reassign' button is visible. A 'Submit' button is highlighted with a red box and a red arrow.

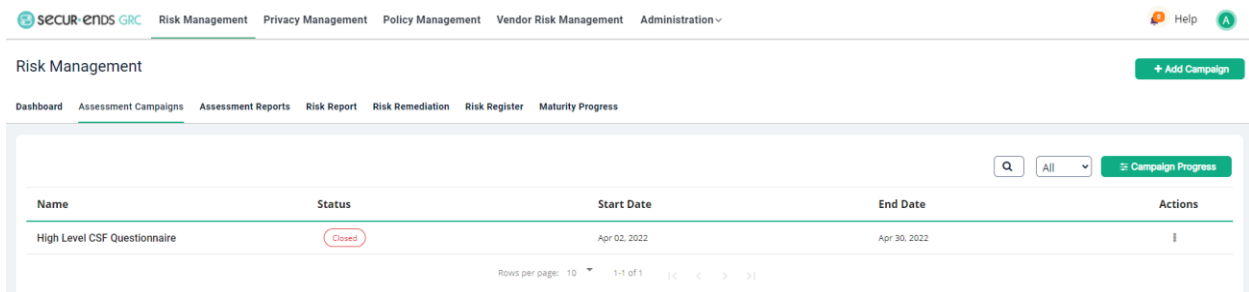
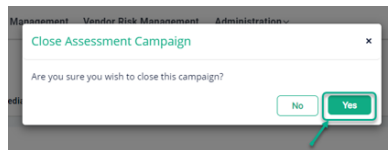
Click the **Back** button.



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

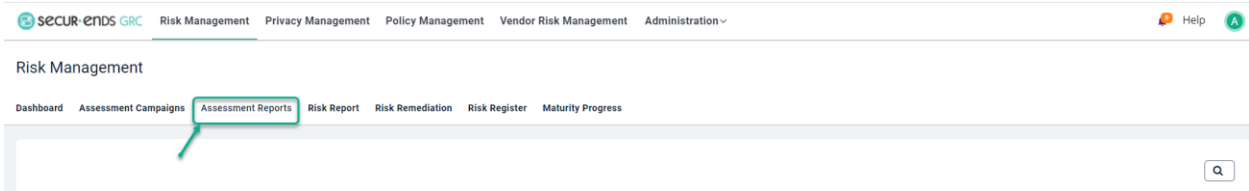


Select **Yes** option to close the campaign.

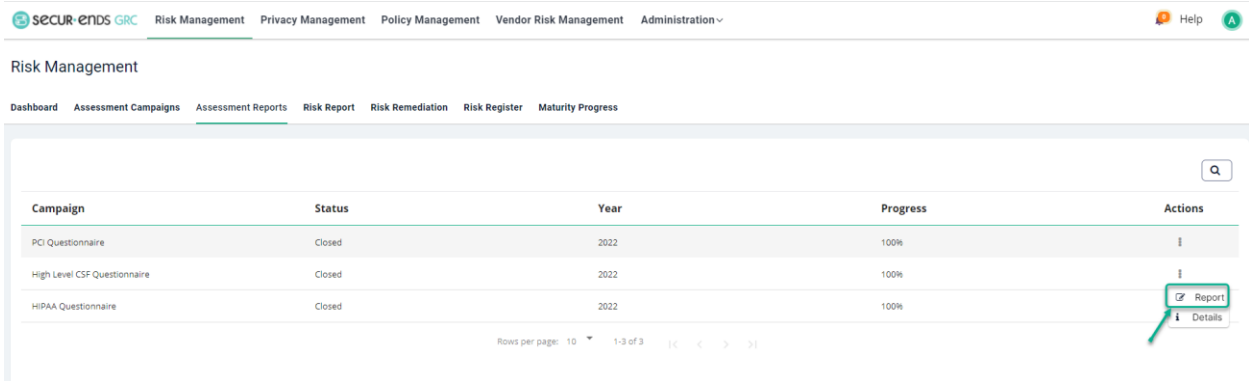


1.3 Assessment Reports

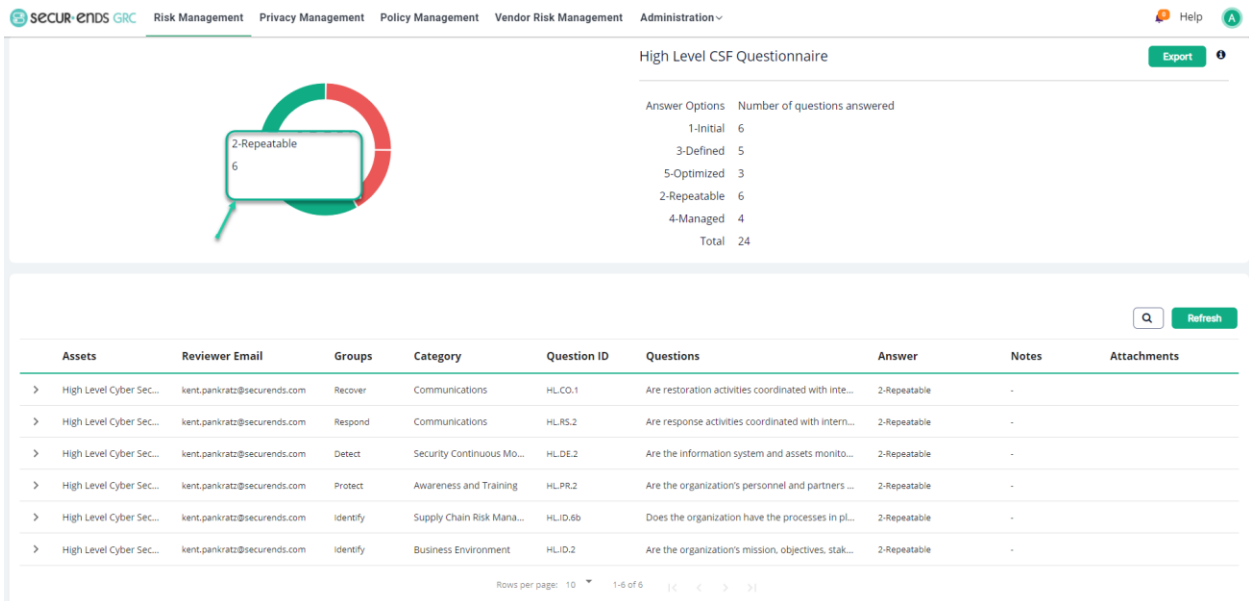
Select the **Risk Management** tab on the main menu and select **Assessment Reports** tab.



Select **Actions** button and select **Report** from the drop-down menu.



Click on a section of the doughnut graphic on the right to view the details of each question answered. The comments and attachments are available for review and export from this page.



1.4 Risk Report

The additional components of the compliance cards and the aggregation tree are visible on the Risk Report dashboard. The selection of completed assessments is also found in the drop-down menu.

Select **Risk Management** tab on the main menu and select **Risk Report** tab.

The screenshot displays the Risk Management dashboard. At the top, there is a navigation bar with 'SECUR-ENDS GRC' and various management tabs. The main content area is divided into several sections: 'Enterprise Security Posture' with a gauge showing risk levels (High, Medium, Low); 'Compliance' with three cards for HIPAA (score 51), PCI (score 51), and SOC 2 Type 2 (score 49); 'Enterprise Security Risk Posture' with a bar chart for the five NIST CSF domains (Identify, Protect, Detect, Respond, Recover); 'Security Profile' showing a SecurEndsGRC Score of 50; and 'Risk Remediation Report' with a search and dropdown menu.

Select a completed assessment from the drop-down list and click the **Generate PDF** button to generate Risk Remediation PDF Report.

The screenshot shows the Risk Remediation Report page. The 'Choose Assessment' dropdown is set to 'High Level CSF Questionnaire'. Below the dropdown is a table with the following data:

Question ID	Question	Answer	Security Posture Score	Risk Remediation
> HL.DE.1	Is anomalous activity detected in a timely manner and the potential L...	1-initial	20	https://nvlpubs.nist.gov/nistpu...
> HL.RS.1	Is analysis conducted to ensure adequate response and support reco...	1-initial	20	https://nvlpubs.nist.gov/nistpu...
> HL.ID.5	Are the organization's priorities, constraints, risk tolerances, and assu...	1-initial	20	https://csrc.nist.gov/publication...

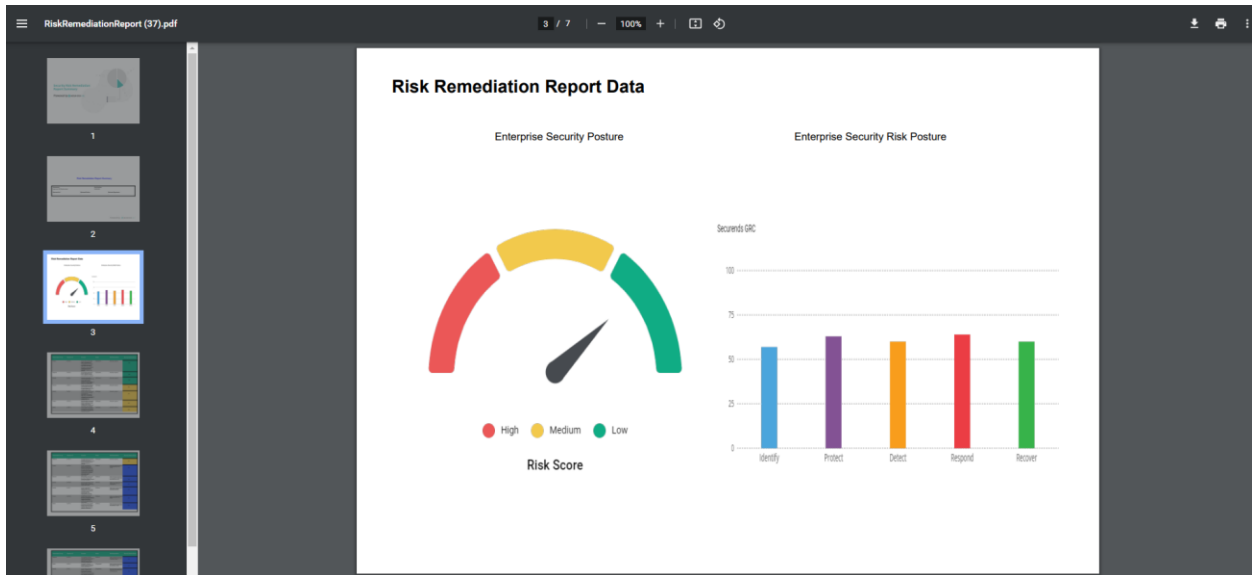
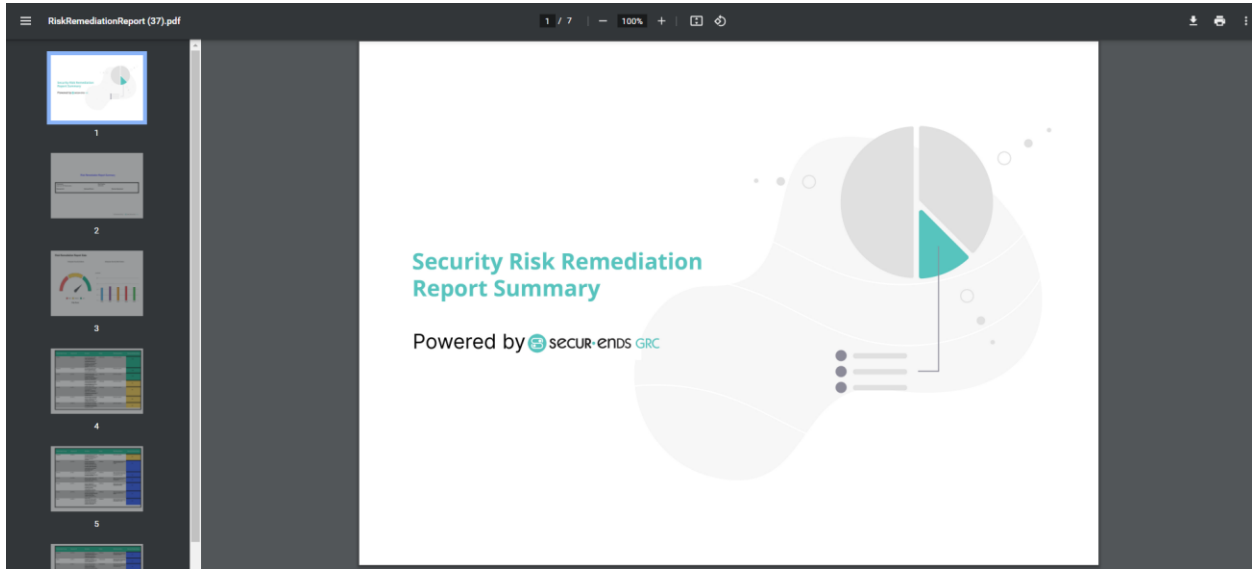
Buttons for 'Export' and 'Generate PDF' are located to the right of the table.

Open or Save the PDF

As shown in the Chrome Browser.

The screenshot shows a Chrome browser address bar with the file path 'RiskRemediationR...pdf' and a 'Show all' button.

As displayed in a PDF reader.



RiskRemediationReport (37).pdf 4 / 7 100%

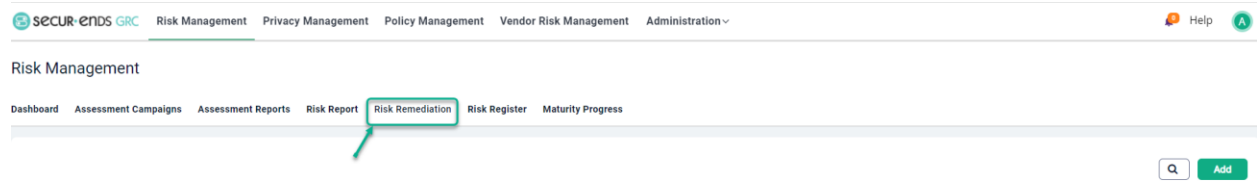
Presentation Group	Question ID	Question	Status	Risk Remediation	Security Posture Score
Protect	HL_PR.4	Are security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures maintained and used to manage protection of information systems and assets?	5-Optimized	No action required.	100
Respond	HL_RS.4	Are activities performed to prevent expansion of an event, mitigate its effects, and eradicate the incident?	5-Optimized	No action required.	100
Identify	HL_ID.4	Does the organization understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals?	5-Optimized	No action required.	100
Recover	HL_RP.1	Are the recovery processes and procedures executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events?	4-Managed	No action required.	80
Identify	HL_ID.3	Are the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements understood and inform the management of cybersecurity risk?	4-Managed	No action required.	80
Protect	HL_PR.3	Are information and records (data) managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information?	4-Managed	No action required.	80
Detect	HL_DE.3	Is the detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events?	4-Managed	No action required.	80

1.5 Risk Remediation

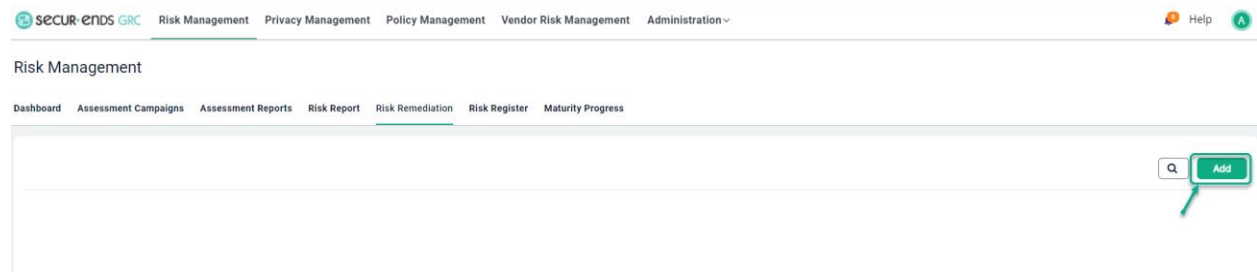
Many of the questions are answered with good performance results. The few that have low scores need to be added to a risk remediation plan. This is the process of creating a list of a few remediation requirements from the larger assessment.

Creation of Remediation Plan

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

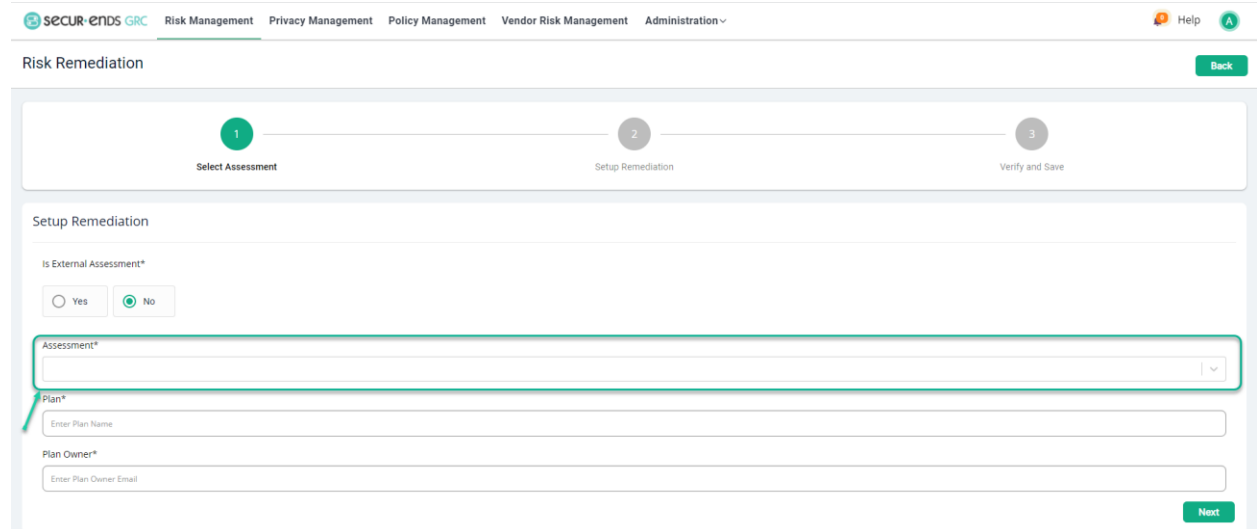


Click the **Add** button to follow three step process.



1.5.1 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*
High Level CSF 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*
High Level CSF Questionnaire

Plan*
High Level CSF Remediation Plan

Plan Owner*
User@securends.com

Next

1.5.2 Step 2: Setup Remediation

Of those items that need to be remediated, select a **Priority** and a choice of **Ticket** actions from the drop-down menu, enter a unique **Remediation Owner** for each row and add the necessary **Comments** to the rows that selected to be included on the report.

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

Help

Selected Assessment: High Level CSF Questionnaire Plan Name: High Level CSF Remediation Plan Plan Owner Email: User@securends.com

Remediation

ID	Presentation Gr...	Questions	Answer	Score	Priority *	Ticket *	Remediation Owner *	Comments	Risk Remediation
> HL.DE.1	Detect	Is anomalous activity detected in a tim...	1-Initial	20	1	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.CO.1	Recover	Are restoration activities coordinated ...	1-Initial	20	4	N	User@securends.com		https://nvlpubs.nist.gov/n
> HL.ID.1	Identify	Are the data, personnel, devices, syste...	1-Initial	20	3	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.ID.6a	Identify	Are the organization's priorities, constr...	1-Initial	20	3	Y	User@securends.com		https://csrc.nist.gov/Proje
> HL.PR.6	Protect	Are technical security solutions manag...	1-Initial	20	2	Y	User@securends.com		https://csrc.nist.gov/publi
> HL.PR.1	Protect	Is access to physical and logical assets ...	1-Initial	20	1	N	User@securends.com		https://csrc.nist.gov/Topic
> HL.ID.6b	Identify	Does the organization have the proces...	2-Repeatable	40	4	Y	User@securends.com		https://csrc.nist.gov/Proje
> HL.ID.2	Identify	Are the organization's mission, objecti...	2-Repeatable	40	2	N	User@securends.com		https://www.nist.gov/cybe
> HL.RS.2	Respond	Are response activities coordinated wit...	2-Repeatable	40	5	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.DE.2	Detect	Are the information system and assets...	2-Repeatable	40	1	N	User@securends.com		https://nvlpubs.nist.gov/n

Rows per page: 10 1-10 of 24

Back Next

Click the **Next** button.

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

Help

Selected Assessment: High Level CSF Questionnaire Plan Name: High Level CSF Remediation Plan Plan Owner Email: User@securends.com

Remediation

ID	Presentation Gr...	Questions	Answer	Score	Priority *	Ticket *	Remediation Owner *	Comments	Risk Remediation
> HL.DE.1	Detect	Is anomalous activity detected in a tim...	1-Initial	20	1	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.CO.1	Recover	Are restoration activities coordinated ...	1-Initial	20	4	N	User@securends.com		https://nvlpubs.nist.gov/n
> HL.ID.1	Identify	Are the data, personnel, devices, syste...	1-Initial	20	3	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.ID.6a	Identify	Are the organization's priorities, constr...	1-Initial	20	3	Y	User@securends.com		https://csrc.nist.gov/Proje
> HL.PR.6	Protect	Are technical security solutions manag...	1-Initial	20	2	Y	User@securends.com		https://csrc.nist.gov/publi
> HL.PR.1	Protect	Is access to physical and logical assets ...	1-Initial	20	1	N	User@securends.com		https://csrc.nist.gov/Topic
> HL.ID.6b	Identify	Does the organization have the proces...	2-Repeatable	40	4	Y	User@securends.com		https://csrc.nist.gov/Proje
> HL.ID.2	Identify	Are the organization's mission, objecti...	2-Repeatable	40	2	N	User@securends.com		https://www.nist.gov/cybe
> HL.RS.2	Respond	Are response activities coordinated wit...	2-Repeatable	40	5	Y	User@securends.com		https://nvlpubs.nist.gov/n
> HL.DE.2	Detect	Are the information system and assets...	2-Repeatable	40	1	N	User@securends.com		https://nvlpubs.nist.gov/n

Next

1.5.3 Step 3: Verify and Save

Click the **Save** button.

The screenshot shows the 'Verify and Save' step of a remediation plan. At the top, a progress bar indicates three steps: 1. Select Assessment, 2. Setup Remediation, and 3. Verify and Save. Below the progress bar, the 'Selected Assessment' is 'High Level CSF Questionnaire', the 'Plan Name' is 'High Level CSF Remediation Plan', and the 'Plan Owner Email' is 'User@secureends.com'. A 'Remediation' table is displayed with columns for Question ID, Presentation Gr..., Questions, Answer, Score, Priority, Ticket, Remediation Owner, Comments, and Risk Remediation. A 'Save' button is highlighted in the top right corner of the table.

Question ID	Presentation Gr...	Questions	Answer	Score	Priority	Ticket	Remediation Owner	Comments	Risk Remediation
> HL.DE.1	Detect	Is anomalous activity detected in a tim...	1-Initial	20	1	Y	User@secureends.com		https://nvlpubs.nist.gov/nistpubs
> HL.CO.1	Recover	Are restoration activities coordinated ...	1-Initial	20	4	N	User@secureends.com		https://nvlpubs.nist.gov/nistpubs
> HL.ID.1	Identify	Are the data, personnel, devices, syste...	1-Initial	20	3	Y	User@secureends.com		https://nvlpubs.nist.gov/nistpubs
> HL.ID.6a	Identify	Are the organization's priorities, constr...	1-Initial	20	3	Y	User@secureends.com		https://csrc.nist.gov/Projects/cybe
> HL.PR.6	Protect	Are technical security solutions manag...	1-Initial	20	2	Y	User@secureends.com		https://csrc.nist.gov/publications/
> HL.PR.1	Protect	Is access to physical and logical assets ...	1-Initial	20	1	N	User@secureends.com		https://csrc.nist.gov/Topics/Secur
> HL.ID.6b	Identify	Does the organization have the proces...	2-Repeatable	40	4	Y	User@secureends.com		https://csrc.nist.gov/Projects/cybe
> HL.ID.2	Identify	Are the organization's mission, objecti...	2-Repeatable	40	2	N	User@secureends.com		https://www.nist.gov/cybersecurit
> HL.RS.2	Respond	Are response activities coordinated wit...	2-Repeatable	40	5	Y	User@secureends.com		https://nvlpubs.nist.gov/nistpubs

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

The screenshot shows the 'Risk Management' page. The 'Risk Remediation' tab is selected. A table lists remediation plans. The 'High Level CSF Remediation Plan' is highlighted. The 'Actions' column for this plan shows a dropdown menu with 'View Report' and 'Delete' options. A 'Save' button is also visible in the top right corner of the table.

Remediation Plan	Plan Owner	Assessment Type	Actions
High Level CSF Remediation Plan	User@secureends.com	Internal	<ul style="list-style-type: none">View ReportDelete

Generate Remediation Plan Report

Click the **Generate PDF** button.

Remediation Plan

Generate PDF Back

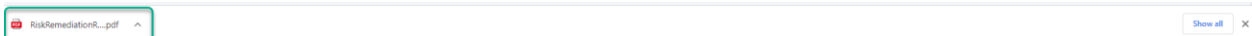
Remediation Details

Plan Name : High Level CSF Remediation Plan
Plan Owner : User@securends.com
Assessment : High Level CSF Questionnaire

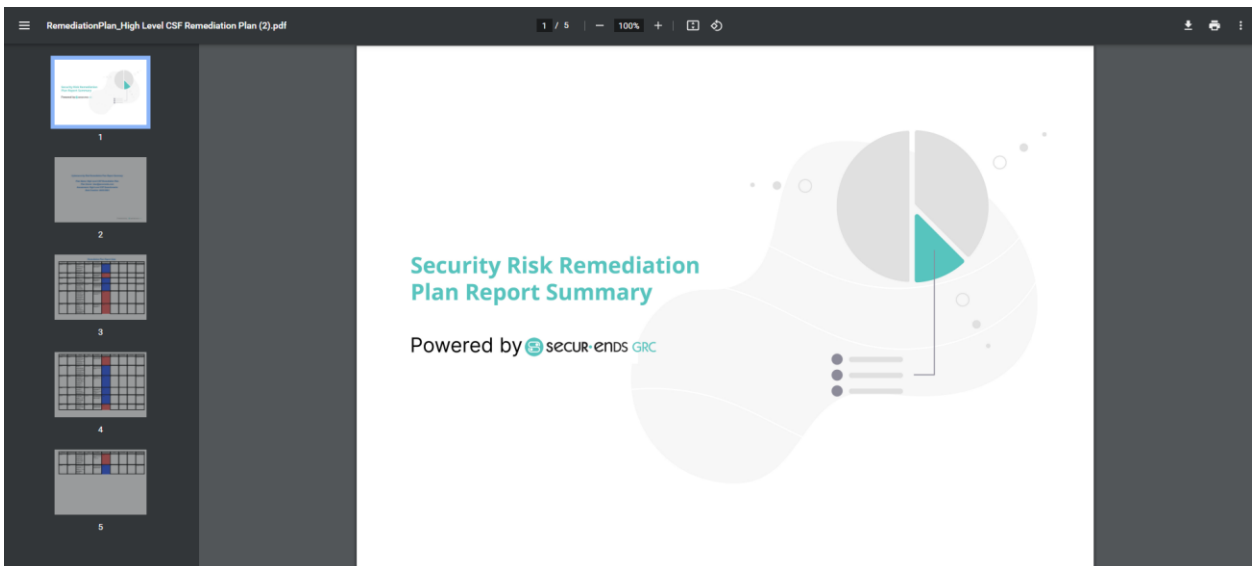
Question ID	Presentation Group	Question	Answer	Security Posture Score	Priority	Ticket	Remediation Owner	Risk Remediation
> HL_DE.1	Detect	Is anomalous activity detected in a timely man...	1-Initial	20	1	Y	User@securends.com	https://nvlpubs.nist.gov/nistpubs/
> HL_PR.1	Protect	Is access to physical and logical assets and ass...	1-Initial	20	1	N	User@securends.com	https://csrc.nist.gov/Topics/Secur
> HL_DE.2	Detect	Are the information system and assets monito...	2-Repeatable	40	1	N	User@securends.com	https://nvlpubs.nist.gov/nistpubs/
> HL_PR.6	Protect	Are technical security solutions managed to en...	1-Initial	20	2	Y	User@securends.com	https://csrc.nist.gov/publications/
> HL_ID.2	Identify	Are the organization's mission, objectives, stak...	2-Repeatable	40	2	N	User@securends.com	https://www.nist.gov/cybersecurit
> HL_ID.3	Identify	Are the policies, procedures, and processes to ...	3-Defined	60	2	Y	User@securends.com	https://csrc.nist.gov/Projects/risk-
> HL_DE.3	Detect	Is the detection processes and procedures mai...	3-Defined	60	2	Y	User@securends.com	https://csrc.nist.gov/CSRC/media/

Open or Save the PDF


As shown in the Chrome browser.



As displayed in a PDF reader.




RemediationPlan_High Level CSF Remediation Plan (2).pdf 2 / 5 100%




Cybersecurity Risk Remediation Plan Report Summary

Plan Name: High Level CSF Remediation Plan
Plan Owner: User@securends.com
Assessment: High Level CSF Questionnaire
Date Creation: 04/03/2022

Powered by 

RemediationPlan_High Level CSF Remediation Plan (2).pdf 3 / 5 100%



Remediation Plan Report Data

Question Id	Presentation Group	Question	Status	Remediation	Security Posture Score	Priority	Ticket Status	Comments	Remediation Owner
HL.RS.2	Respond	Are response activities coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement?	2-Repeatable	https://nvlpubs.nist.gov/nvlpubs/SpecialPublications/NIST.SP.800-150.pdf	85	5	Y		User@securends.com
HL.CO.1	Recover	Are restoration activities coordinated with internal and external parties?	1-Initial	https://nvlpubs.nist.gov/nvlpubs/SpecialPublications/NIST.SP.800-150.pdf	20	4	N		User@securends.com
HL.ID.65	Identify	Does the organization have the processes in place to identify, assess and manage supply chain risks?	2-Repeatable	https://oig.dhs.gov/Reports-and-Testimony/Reports-and-Testimony/2021/03/2021-017-Report-to-Congress-on-Cybersecurity-Supply-Chain-Risk-Management	85	4	Y		User@securends.com
HL.RS.3	Respond	Are operational response activities improved by incorporating lessons learned from current and previous detection, response activities?	3-Defined	https://nvlpubs.nist.gov/nvlpubs/Legacy/SP/nist.sp.pdf/athor800-341.pdf	90	4	N		User@securends.com
HL.ID.1	Identify	Are the orgs, personnel, devices, systems, and services that enable the organization to achieve business purposes identified and managed consistent with their relative importance to business and the organization's risk strategy?	1-Initial	https://nvlpubs.nist.gov/nvlpubs/SpecialPublications/NIST.SP.1800-5.pdf	20	3	Y		User@securends.com
HL.ID.64	Identify	Are the organization's processes, constraints, risk tolerances, and assumptions established and used to support risk decisions associated with managing supply chain risks?	1-Initial	https://oig.dhs.gov/Reports-and-Testimony/Reports-and-Testimony/2021/03/2021-017-Report-to-Congress-on-Cybersecurity-Supply-Chain-Risk-Management	20	3	Y		User@securends.com

1.6 Risk Register

A method of communication to the Enterprise Risk Management team is incorporated in the Risk Register. The content of the page is derived from the NISTIR 8286B document for gathering and prioritizing of IT cybersecurity risks for delivering to executive management for resolution actions.

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

Risk Register

ID	Source Assessment	Assessment Type	Remediation Date	Question Id	Priority	Presentation Group	Control Set Group	Risk Category	Financial Impact
1	High Level CSF Remediation ...	Internal	Apr 02 2022	HL_DE.1	1	Detect	NIST CSF 1.1	Anomalies and Events	Select
2	High Level CSF Remediation ...	Internal	Apr 02 2022	HL_CO.1	4	Recover	NIST CSF 1.1	Communications	Select
3	High Level CSF Remediation ...	Internal	Apr 02 2022	HL_ID.1	3	Identify	NIST CSF 1.1	Asset Management	Select
4	High Level CSF Remediation ...	Internal	Apr 02 2022	HL_ID.6a	3	Identify	NIST CSF 1.1	Supply Chain Risk Managem...	Select
5	High Level CSF Remediation ...	Internal	Apr 02 2022	HL_PR.6	2	Protect	NIST CSF 1.1	Protective Technology	Select

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

Risk Register

Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Status
Anomalies and Events	Select	Select	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select
Communications	Select	Select	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select
Asset Management	Select	Select	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select

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

Risk Register

act	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Status	Expected Date	ERM Priority
)	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select		Select
)	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select		Select
)	Select	Select	Select	https://mlpubs.nist.gov/nistpubs/	User@securends.com	Select		Select

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

The screenshot shows the 'Risk Register' page in the SecurEnds GRC system. A dropdown menu is open, showing options to hide or show columns. The 'ID' column is currently hidden, as indicated by the unchecked checkbox. The other columns shown in the table are Source Assessment, Remediation Date, Question Id, and Priority.

ID	Source Assessment	Assessment Type	Remediation Date	Question Id	Priority	Presentation Group	Control Set	Financial Impact
1	High Level CSF Remediation ...	Internal	Apr 02 2022	HL.DE.1	1	Detect	NIST CSF 1.1	Select
2	High Level CSF Remediation ...	Internal	Apr 02 2022	HL.CO.1	4	Recover	NIST CSF 1.1	Select
3	High Level CSF Remediation ...	Internal	Apr 02 2022	HL.ID.1	3	Identify	NIST CSF 1.1	Select

Select the columns that are presented in the report.

The screenshot shows the 'Risk Register' page with the dropdown menu open. The 'Source Assessment' and 'Remediation Date' columns are selected, as indicated by the checked checkboxes. The 'ID' column remains hidden. The table now includes 'Financial Impact' and 'Assessment Likelihood' columns.

ID	Question Id	Priority	Presentation Group	Control Set Group	Risk Category	Financial Impact	Impact	Assessment Likelihood
1	HL.DE.1	1	Detect	NIST CSF 1.1	Anomalies and Events	Select	Select	Select
2	HL.CO.1	4	Recover	NIST CSF 1.1	Communications	Select	Select	Select
3	HL.ID.1	3	Identify	NIST CSF 1.1	Asset Management	Select	Select	Select

Click the Save button.

The screenshot shows the 'Risk Register' page with the 'Save' button highlighted. The table now includes 'Reputation Impact', 'Mission Impact', and 'Exposure Rating' columns. The 'Assessment Likelihood' column is also present.

ID	Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating
1	HL.DE.1	1	Detect	Anomalies and Events	Low	Low	Low	Low	2
2	HL.CO.1	4	Recover	Communications	Medium	High	Medium	Medium	4
3	HL.ID.1	3	Identify	Asset Management	Low	Not Applicable	Not Applicable	Low	5

Generate a Remediation Plan Report

Click the **Generate PDF Report** button.

Risk Register

ID	Question Id	Priority	Presentation Group	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating
1	HL.DE.1	1	Detect	Anomalies and Events	Low	Medium	High	Medium	2
2	HL.RS.1	4	Respond	Analysis	High	Medium	Medium	High	6
3	HL.ID.5	3	Identify	Risk Management Strategy	Not Applicable	High	Low	Medium	10

Open or Save PDF Report

As shown in the Chrome browser.

As displayed in a PDF reader.

Risk Register Report (9).pdf

1 / 3 | 100% | [Print] [Share]

Security Risk Remediation Report Summary

Powered by secur:ends GRC

Risk Register Report (9).pdf 2 / 3 100%

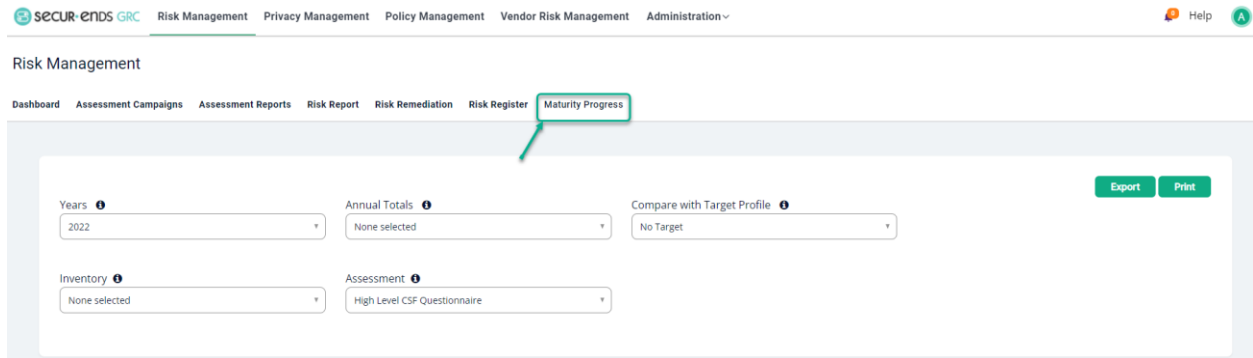
Risk Register Report

ID	Assessment Type	Question ID	Priority	Prevention Stage	Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Response	Risk Owner	Expected Date	Status	ERM Priority
1	Internal	HL.DE.1	1	Detect	Anomalies and Events	Low	Low	Low	Low	2	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-30	Pending	Low
2	Internal	HL.CO.1	4	Recover	Communications	Medium	High	Medium	Medium	4	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-30	In Progress	Low
3	Internal	HL.ID.1	3	Identify	Asset Management	Low	Not Applicable	Not Applicable	Low	5	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-30	Completed	High
4	Internal	HL.ID.6a	3	Identify	Supply Chain Risk Management	High	Low	Low	Medium	1	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-30	No Actions Required	Medium
5	Internal	HL.PR.6	2	Protect	Protective Technology	Not Applicable	Not Applicable	Medium	High	8	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-27	Pending	Not Applicable
6	Internal	HL.PR.1	1	Protect	Identity Management and Access Control	Low	Medium	Medium	Low	7	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-21	In Progress	Low
7	Internal	HL.ID.6b	4	Identify	Supply Chain Risk Management	Medium	High	High	High	3	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-15	No Actions Required	Medium
8	Internal	HL.ID.2	2	Identify	Business Environment	Medium	High	Low	High	9	https://www.secureness.com/secureness-information-security	User@secu-ends.com	2022-04-28	Completed	High
9	Internal	HL.RS.2	5	Respond	Communications	Medium	Medium	Low	Low	10	https://nvd.nist.gov/publications/details.cfm?pubid=819013	User@secu-ends.com	2022-04-29	Completed	Low

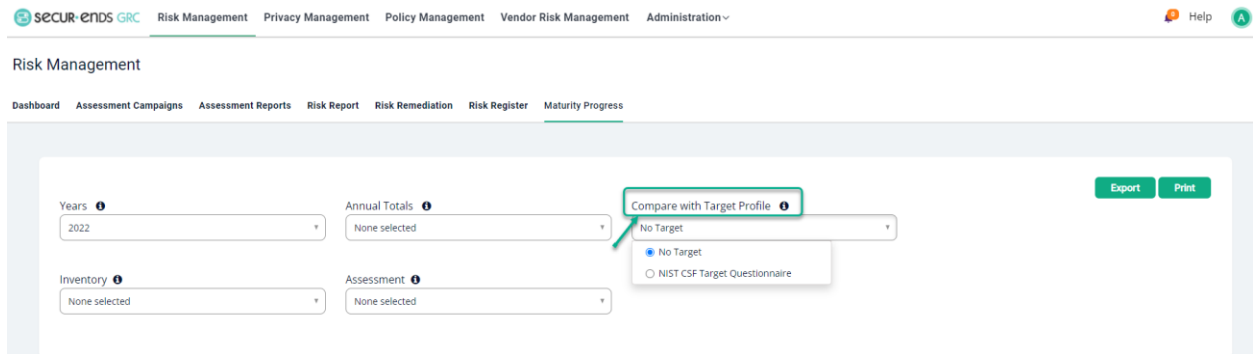
1.7 Maturity Progress

The comparison of the current assessments with a target profile assessment is found within the Maturity Progress page.

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



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



Select a dropdown option of **Years**, **Annual totals**, **Inventory**, or **Assessment** for the comparison of current assessments with the Target Profile.

The screenshot displays the SecurEnds GRC interface with the following elements:

- Navigation Bar:** secur-ends GRC | Risk Management | Privacy Management | Policy Management | Vendor Risk Management | Administration
- Filters:**
 - Years:** 2022
 - Annual Totals:** None selected
 - Compare with Target Profile:** NIST CSF Target Questionnaire
 - Inventory:** None selected
 - Assessment:** High Level CSF Questionnaire
- Buttons:** Export, Print
- Chart:** High Level CSF Questionnaire. A grouped bar chart comparing current performance (left bar) against a target (right bar) for five CSF domains: Identify, Protect, Detect, Respond, and Recover. The y-axis ranges from 0 to 100.

CSF Domain	Current Performance (%)	Target Performance (%)
Identify	~65	~50
Protect	~55	~45
Detect	~60	~40
Respond	~55	~60
Recover	~55	~55

[End of Risk Management User Guide]