



Administration User Guide



Table of Contents

Overview.....	2
1 Administration	3
1.1 User Management	3
1.2 Business Hierarchy	5
1.3 Questionnaire.....	7
1.4 Assignment Roles	9
1.5 Inventory.....	10
1.6 Assessment Templates.....	14
1.7 External Assessment	17
1.8 Configuration	19

Product Version	Document Revision	Date
SecurEnds GRC Administration User Guide 1.0	1.0	April 17, 2022

Overview

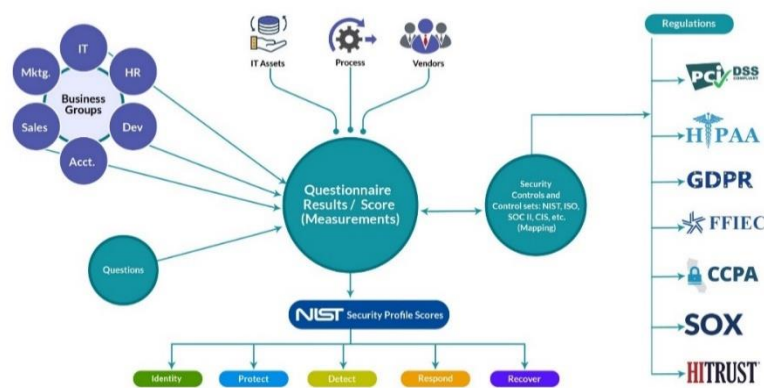
This Administration User Guide outlines the steps to conduct a campaign and produce reports. The steps go through the process of creating an asset within the business hierarchy and associating questions to conduct a campaign which results in an assessment report. The experience of completing the steps 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 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.

1 Administration

Utilize the administration menus to customize and configure each organizations environment.

1.1 User Management

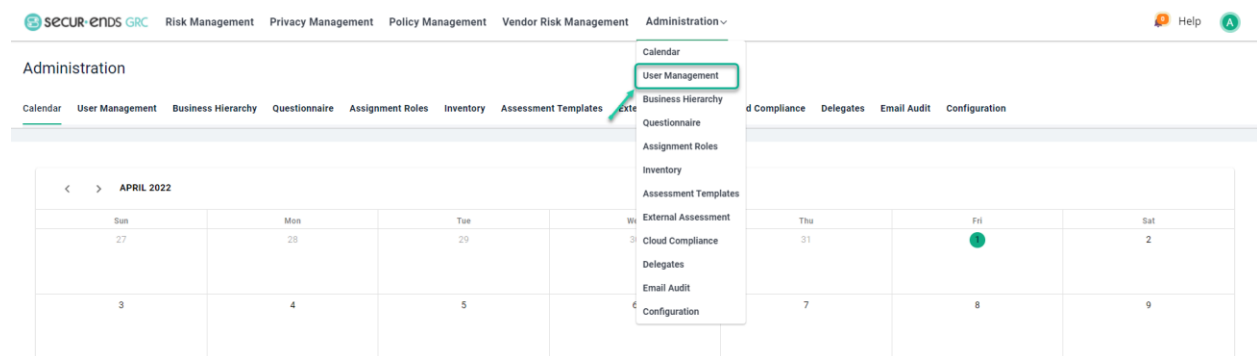
Add users with authentication and authorization to components of the platform.

Users Setup

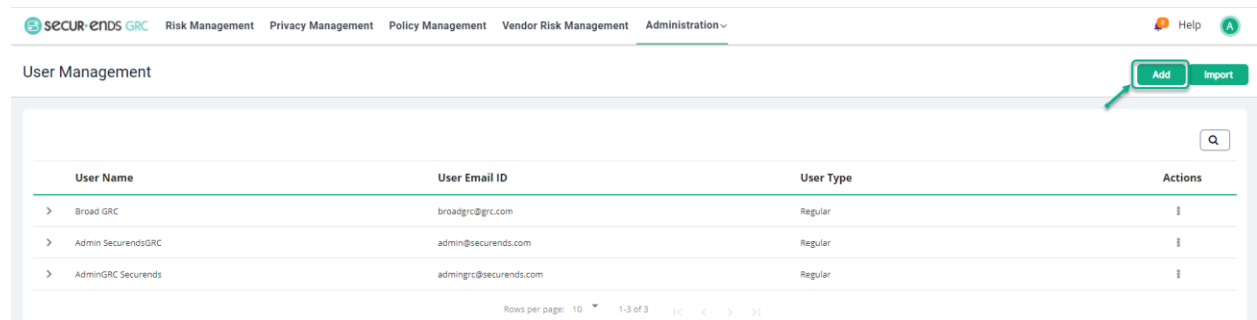
Select **Administration** tab on the main menu.



Select User **Management** from the drop-down list.



Click the **Add** button.



Enter User information and click the **Create** button.

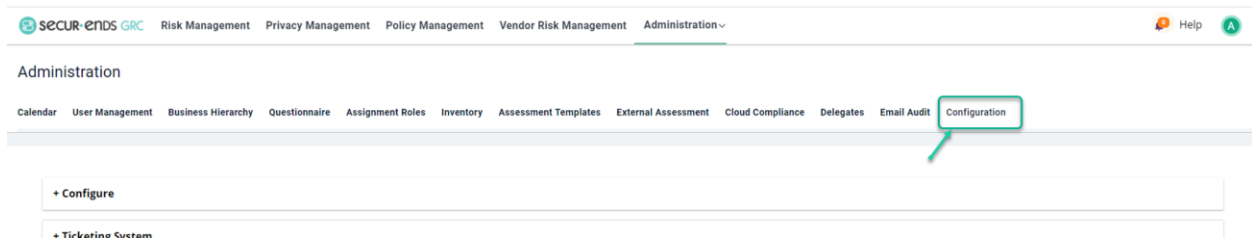
The 'Add User' form contains the following fields:

- User First Name *
- User Middle Name
- User Last Name *
- User Email ID *
- Manager Email ID
- User Title
- Department
- Group Owner
- Location
- Hire Date
- Termination Date

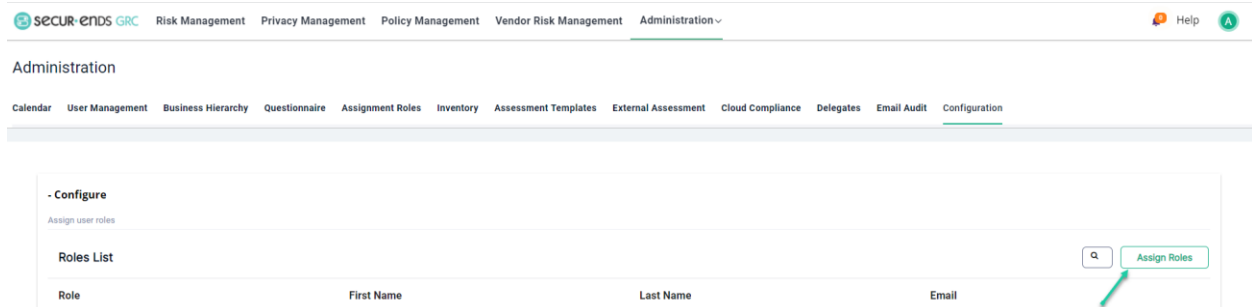
The **Create** button is highlighted with a green box and a callout arrow. Below the form is a green bar with the text **+Add Attributes**.

Assigning Roles to the Users

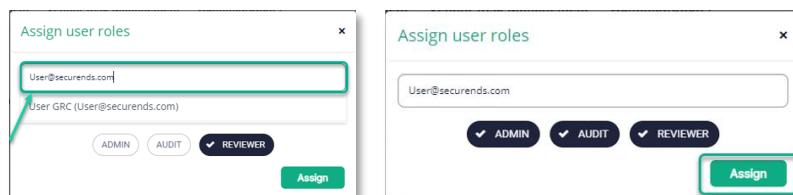
Click the **Configuration** tab in **Administration**.



Select **Configure** option and click the **Assign Roles** button.



Provide Name or Email ID to assign Roles and then select Roles and click the **Assign** button.

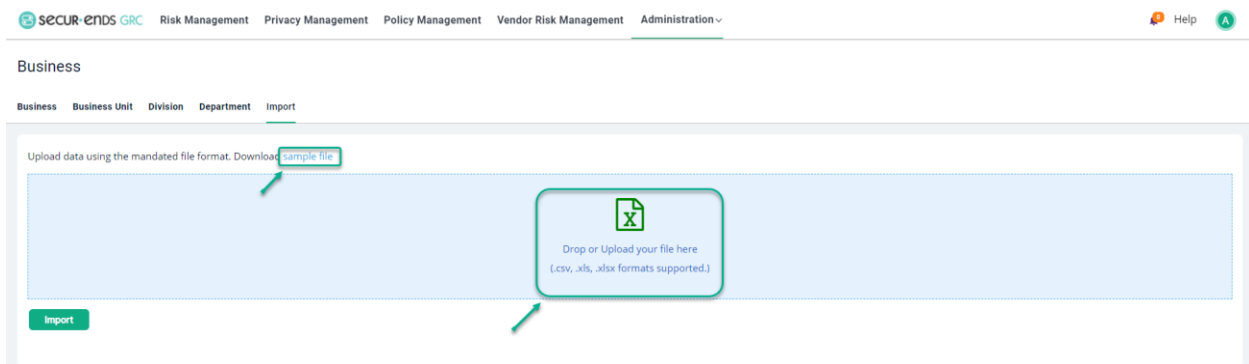
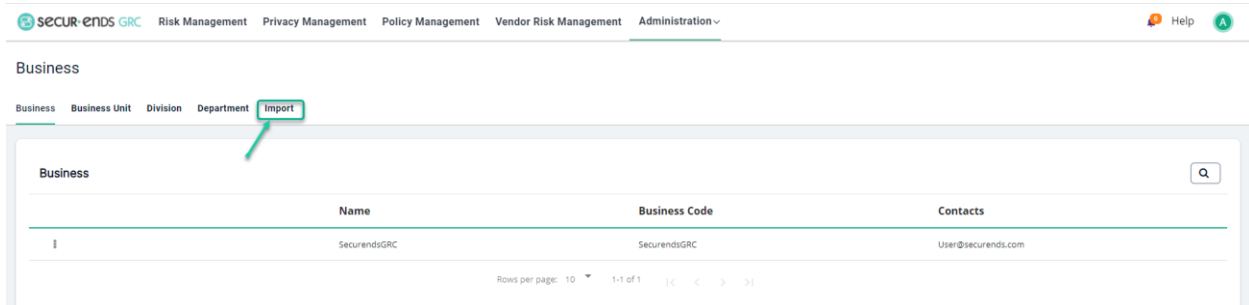


1.2 Business Hierarchy

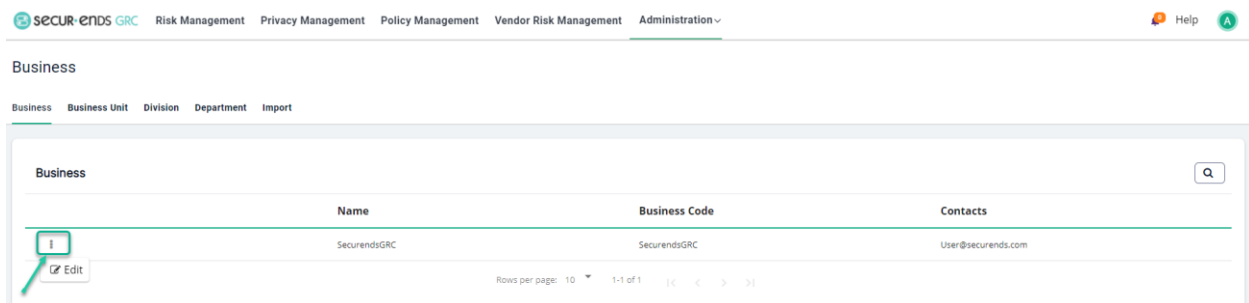
The structure of the tree can be configured to match the organization or as a logical structure to define the areas where assessments need to be categorized. For example, a PCI Cardholder Data Environment (CDE) can be added to the business hierarchy to identify the measurements within the CDE. This structure may be different than the reporting structure but will provide a quick review of PCI scores.

Use the top-level business using Import option.

Select the **Business Hierarchy** in **Administration** drop-down list and click the **Import** tab, download the sample file, edit and upload the file.



Click the **Action** menu button to edit the business name.



Add a business structure manually for each category of Business Unit, Division, or Department.

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

Business

Business Business Unit Division Department Import

Business Unit

Business Name	Name	Unit Code	Contacts	Actions
SecurendsGRC	North America Region	NA	User@securends.com	

Rows per page: 10 1-1 of 1

Q Add Business Unit

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

Business

Business Business Unit Division Department Import

Business Division

Business Hierarchy	Name	Division Code	Contacts	Actions
SecurendsGRC -> North America Region	Division 1	DV	User@securends.com	

Rows per page: 10 1-1 of 1

Q Add Business Division

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

Business

Business Business Unit Division Department Import

Business Department

Business Hierarchy	Name	Department Code	Contacts	Actions
SecurendsGRC -> North America Region -> Division 1	IT Department	IT	User@securends.com	

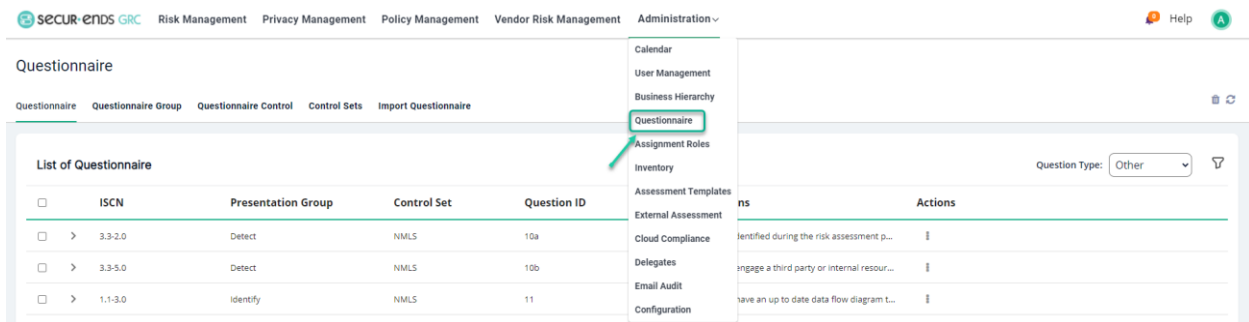
Rows per page: 10 1-1 of 1

Q Add Business Department

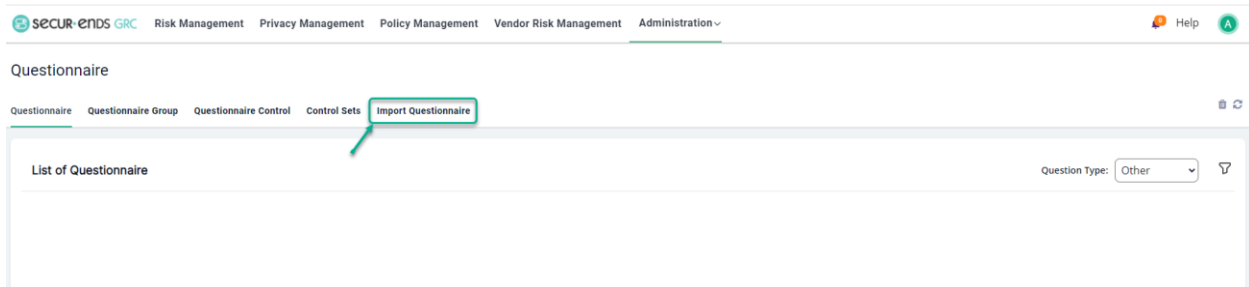
1.3 Questionnaire


The database of security controls and associated questions is maintained within the Questionnaire menu structure.

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

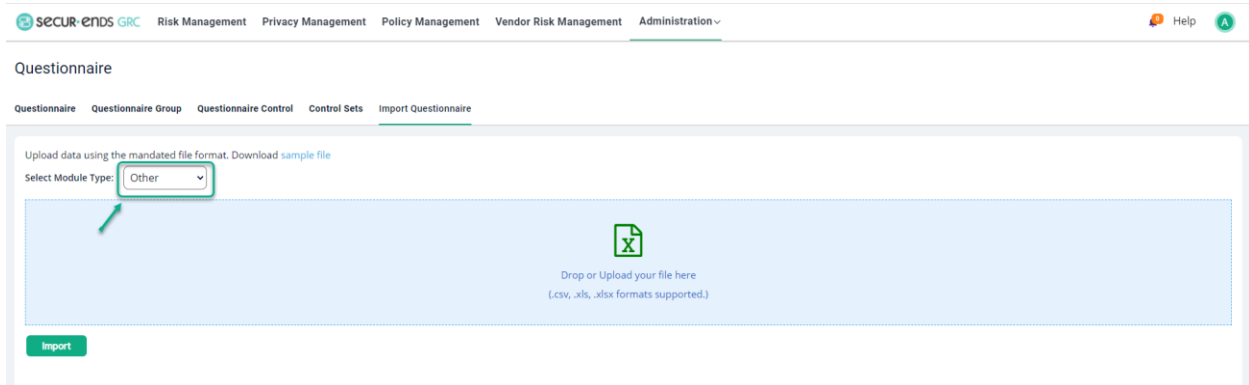


Click the **Import Questionnaire** button.

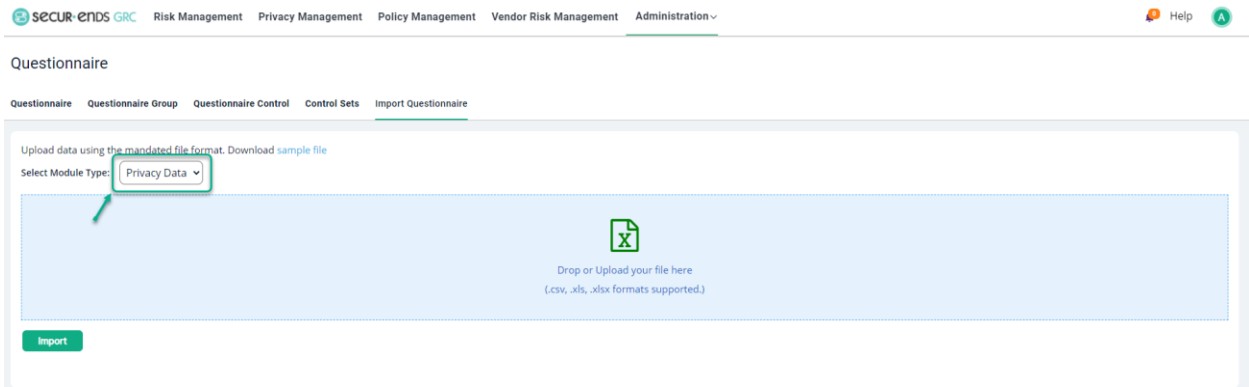


 Select Module type **“Other”** for Risk Management, Vendor Risk Management Questionnaire and select Module type **“Privacy Data”** for Privacy Management Questionnaire.

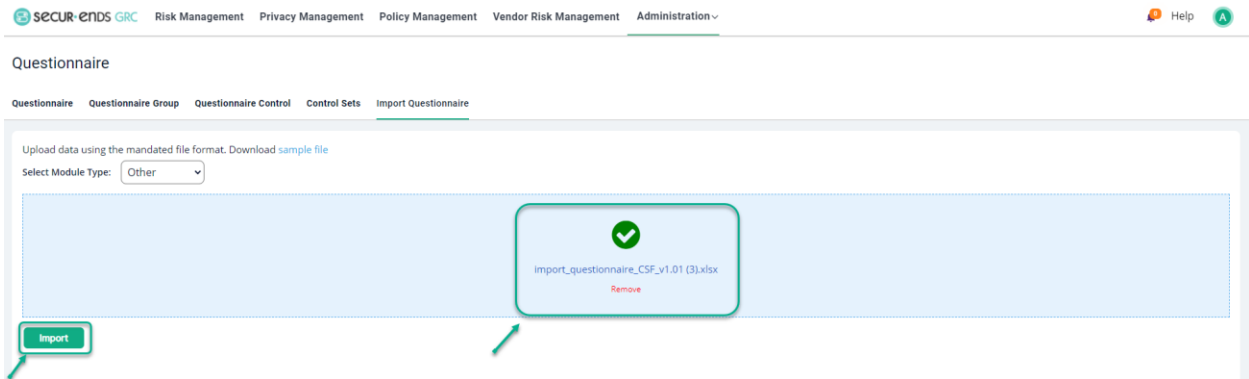
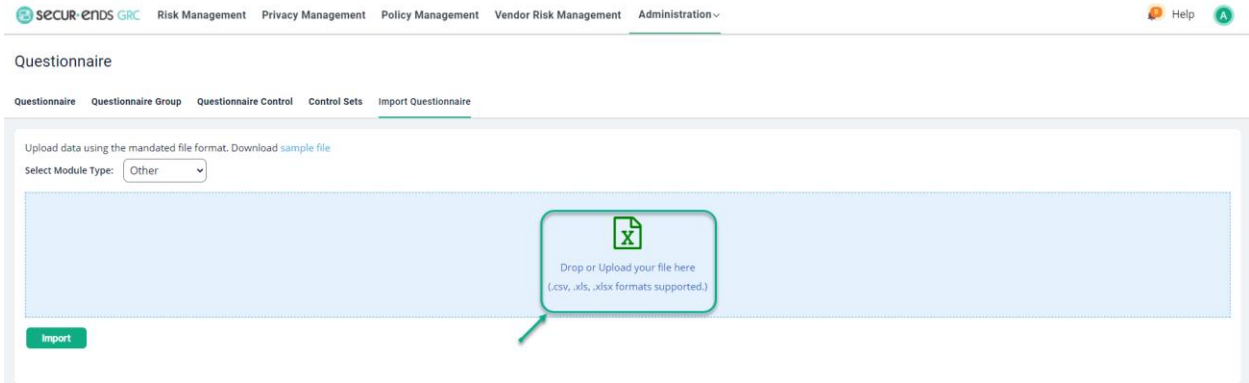
Other



Privacy Data



Drop or Upload Questionnaire file and click the **Import** button.

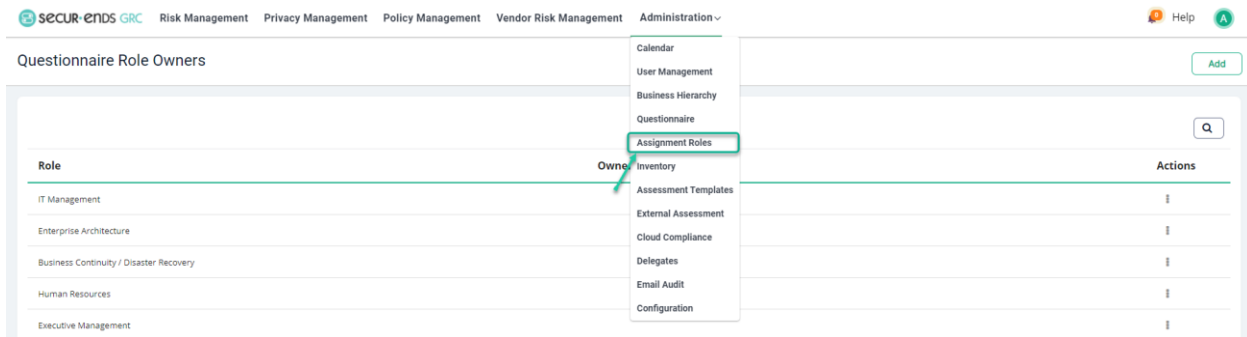


1.4 Assignment Roles

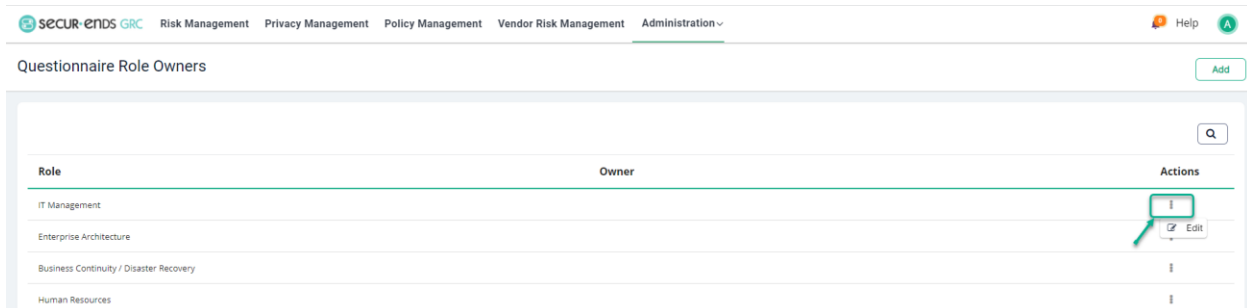
A table of roles within the organization is maintained with the associated users or groups assigned to those roles. This table is applied to assessments when compiled with questions that are relevant to the assigned roles.

Assign Owner to the Roles

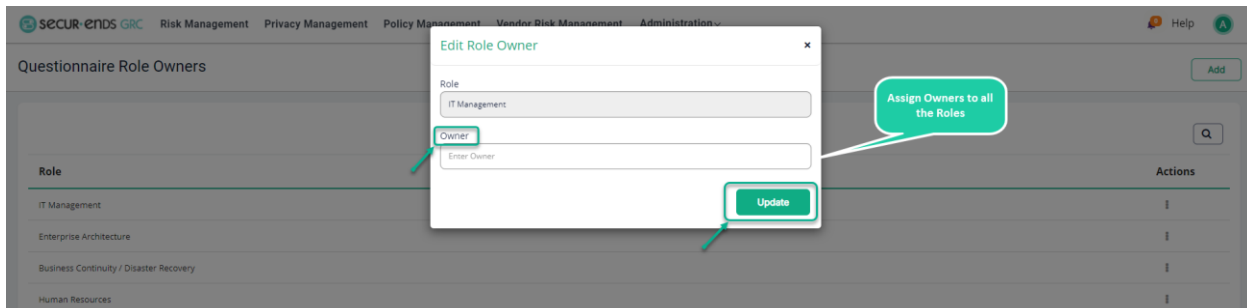
Select the **Assignment Roles** option in **Administration** drop-down list.



Click the **Actions** button to **Edit**.



Enter **Owner** and click the **Update** button.

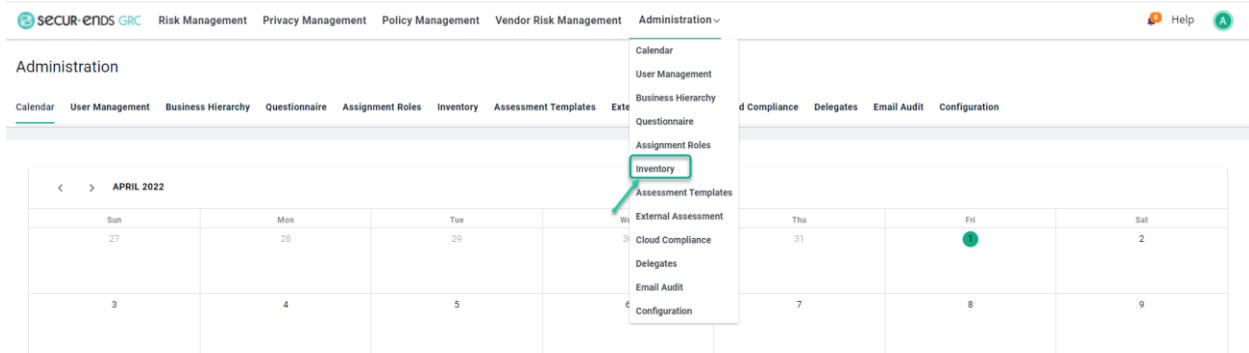


1.5 Inventory

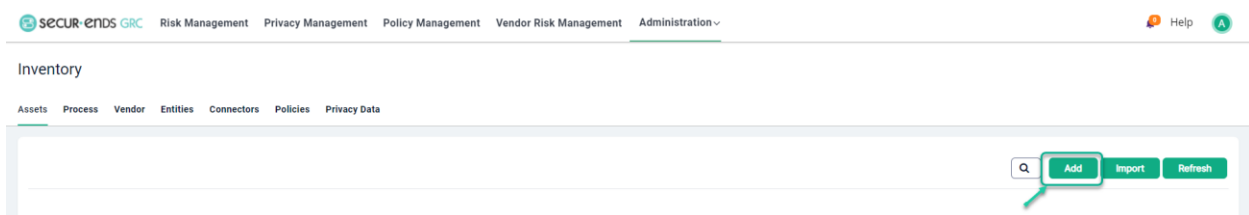
The list of inventory items covers specific physical or logical assets, processes that include information across many assets, entities containing all types of inventories, or categorized as vendors content. Privacy and other inventory must be categorized separately to conform with the assessment requirements.

Add an **Asset/Process/ Entities** under the **Inventory**

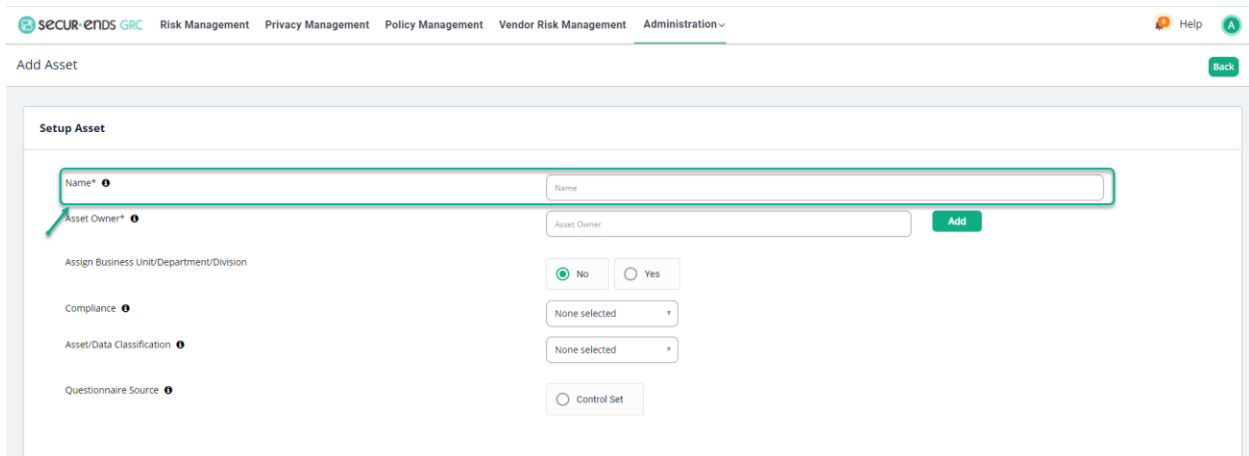
Select the **Inventory** option in **Administration** drop-down list.



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



Name the Asset.



Assign an **Asset 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 Asset Back

Setup Asset

Name* High Level Cyber Security Assessments(NIST CSF)

Asset Owner* Asset Owner Add

Assign Business Unit/Department/Division No Yes

Compliance None selected

Asset/Data Classification None selected

Questionnaire Source Control Set

Assign it to a level within the Business Hierarchy.

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

Add Asset Back

Setup Asset

Name* High Level Cyber Security Assessments(NIST CSF)

Asset Owner* User@securends.com Add

Assign Business Unit/Department/Division No Yes

Compliance None selected

Asset/Data Classification None selected

Questionnaire Source Control Set

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

Setup Business

Business Unit Select Business Division Select Business Department Select

Save

Example:

Setup Business

Business Unit North America Region Business Division Division 1 Business Department IT Department

Save

Select **Compliance** from the drop-down list.

The screenshot shows the 'Setup Asset' form in the SECUR-ENDS GRC system. The form includes fields for Name, Asset Owner, Assign Business Unit/Department/Division, Compliance, Asset/Data Classification, and Questionnaire Source. The 'Compliance' field is highlighted with a red box, and a dropdown menu is open showing options like 'Select all', 'PCI', 'HIPAA', and 'FRIEC'. A red arrow points to the 'Compliance' label.

Select of **Questionnaire Source**

Click the **Control Set** radio button.

The screenshot shows the 'Setup Asset' form in the SECUR-ENDS GRC system. The 'Control Set' radio button is highlighted with a red box, and a red arrow points to it. The form includes fields for Name, Asset Owner, Assign Business Unit/Department/Division, Compliance, Asset/Data Classification, and Questionnaire Source.

Select box for NIST CSF 1.1

The screenshot shows the 'Administration' page in the SecurEnds GRC system. The page title is 'High Level Cyber Security Assessments(NIST CSF)'. The 'Asset Owner*' field is populated with 'User@securends.com'. The 'Assign Business Unit/Department/Division' field has radio buttons for 'No' (selected) and 'Yes'. The 'Compliance' field has a dropdown menu with 'None selected'. The 'Asset/Data Classification' field also has a dropdown menu with 'None selected'. The 'Questionnaire Source' field has a radio button for 'Control Set' (selected) and a list of other options: 'NIST CSF 1.1' (checked), 'Critical Security Controls 6', 'FRIEC (Multiple Choice)', 'FRIEC (Yes/No)', and 'HIPAA Security Rule'. A green arrow points to the 'NIST CSF 1.1' checkbox.

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

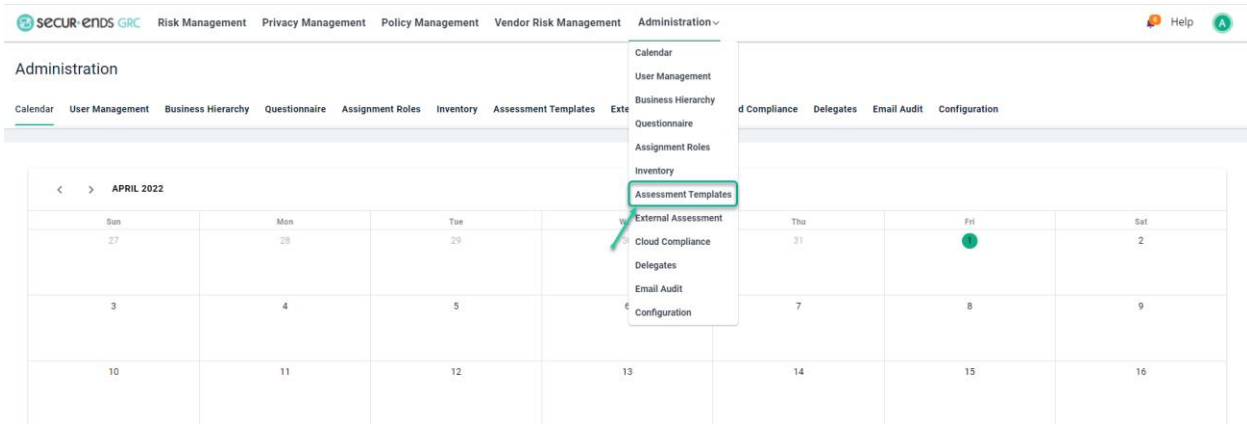
The screenshot shows the 'Administration' page in the SecurEnds GRC system. The page title is 'High Level Cyber Security Assessments(NIST CSF)'. The 'Control Set' field has a radio button for 'Control Set' (selected) and a list of other options: 'NIST CSF 1.1' (checked), 'Critical Security Controls 6', 'FRIEC (Multiple Choice)', 'FRIEC (Yes/No)', 'HIPAA Security Rule', 'NIST SP 800-53r5', 'NIST SP 800-171r2', 'NMLS', 'NYSED 2021', 'PCI DSS 3.2', 'Ransomware', 'AICPA TSC 2017 (SOC)', 'SIGlite-NCSF', 'AWS Cloud Platform', and 'OKta'. Below the list are four input fields: 'Identify', 'Protect', 'Detect', and 'Respond', each with a dropdown menu and a close button. A green arrow points to the 'Save' button in the bottom right corner.

1.6 Assessment Templates

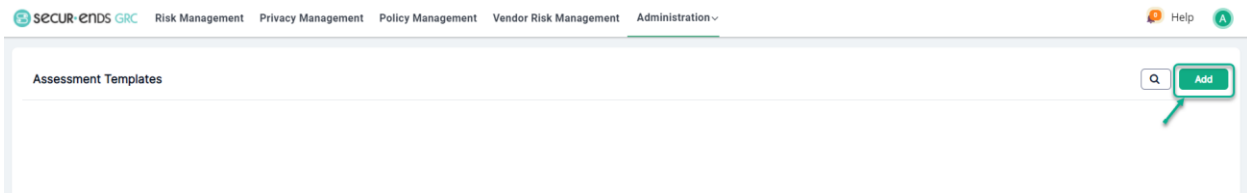
The accumulation of questions and inventory is captured in a template. This layer of configuration adds flexibility to the measurement of risk throughout the organization. Utilize templates to craft a set of questions and controls for efficient processing of campaigns and risk reporting.

Create Assessment Template

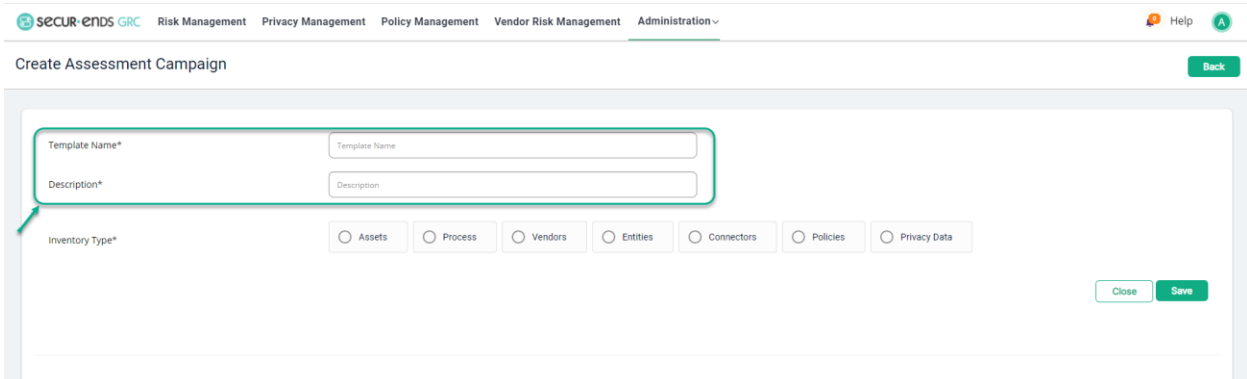
Select the **Assessment Templates** option in **Administration** drop-down list.



Click the **Add** button to create Assessment Template.



Enter a **Template name** and **Description**.



Click the **Assets** radio button and select the asset from the dropdown list.

The screenshot shows the 'Create Assessment Campaign' form. The 'Inventory Type*' field has the 'Assets' radio button selected. The 'Assets' dropdown menu is open, showing a search bar and a list of assets. The asset 'High Level Cyber Security Assessments(NIST CSF)' is selected. The 'Assets' table below has a 'Yes' radio button selected for the selected asset. The 'Actions' column has a 'View Questionnaire' button.

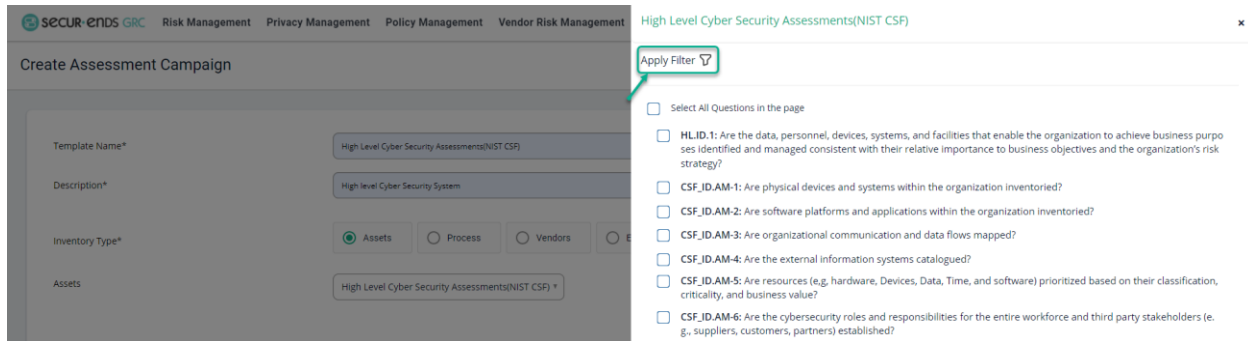
Click the **Yes** radio button to select all questions

or

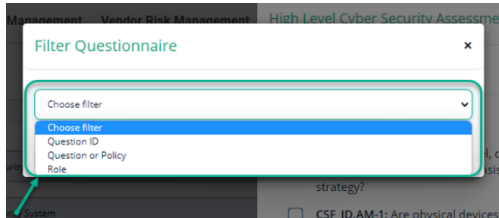
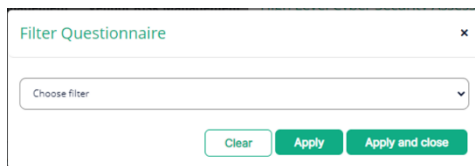
Click the **No** radio button and then click the **Select/Unselect Questionnaire** button.

The screenshot shows the 'Create Assessment Campaign' form. The 'Inventory Type*' field has the 'Assets' radio button selected. The 'Assets' dropdown menu is closed. The 'Assets' table below has the 'No' radio button selected for the asset 'High Level Cyber Security Assessments(NIST CSF)'. The 'Actions' column has a 'Select/Unselect Questionnaire' button highlighted.

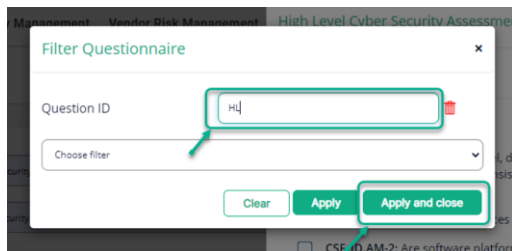
Click the **Apply Filter** symbol.



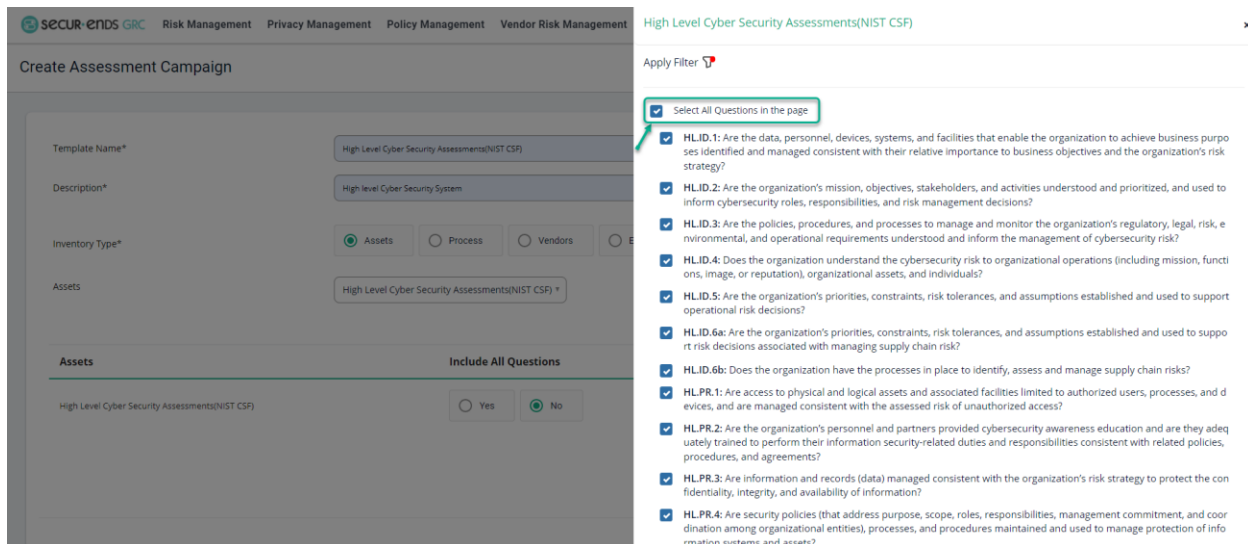
At the pop-up of the filter window, choose **Filter Question ID/ Question or Policy / Role**.



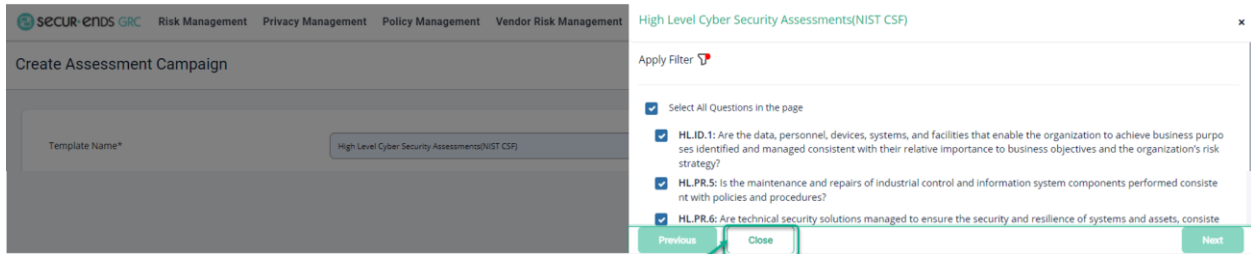
Enter **Question ID** and then click on **Apply and Close** button.



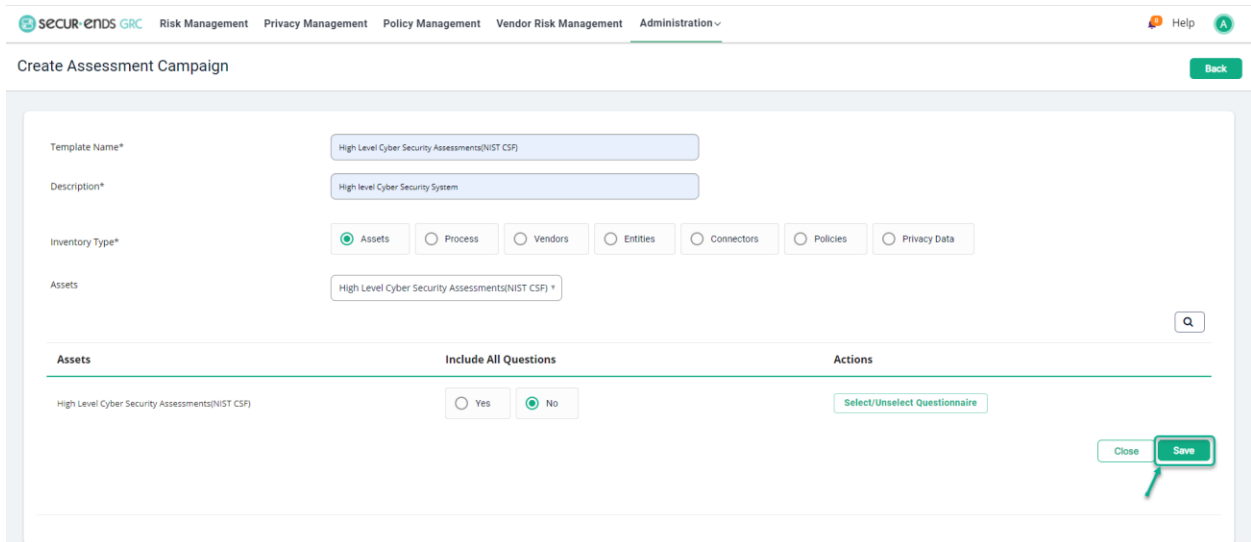
Check the box for **Select All Questions in the page**.



Click the **Close** button.

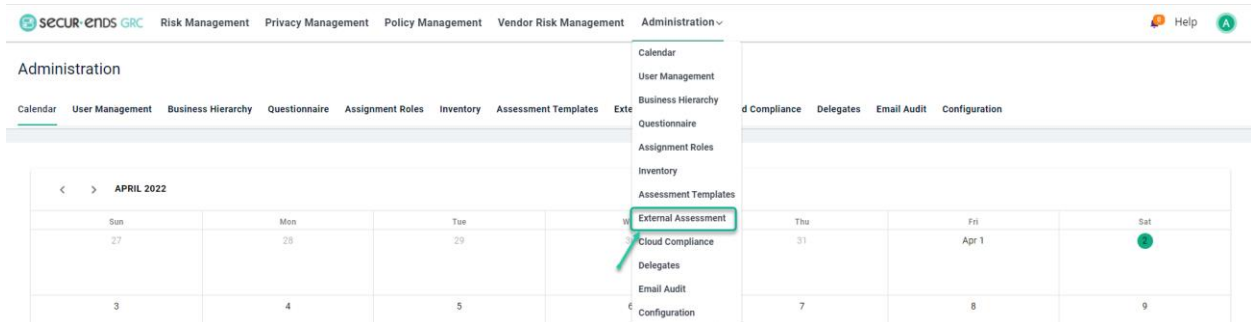


Click the **Save** button.

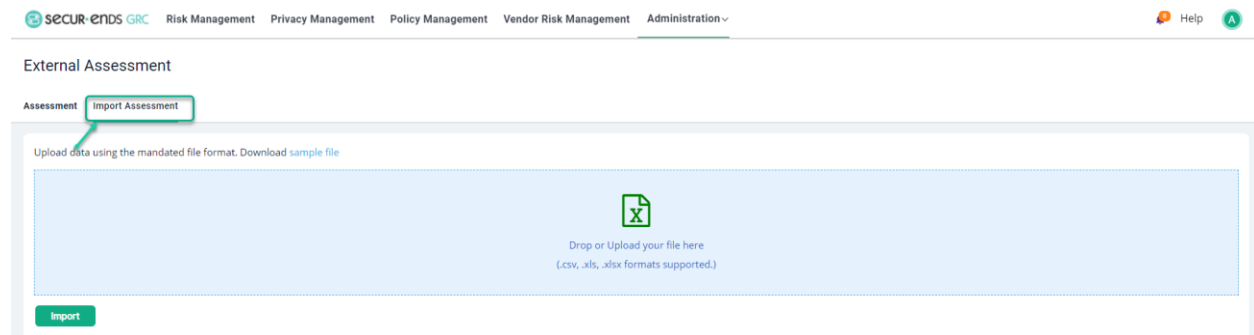


1.7 External Assessment

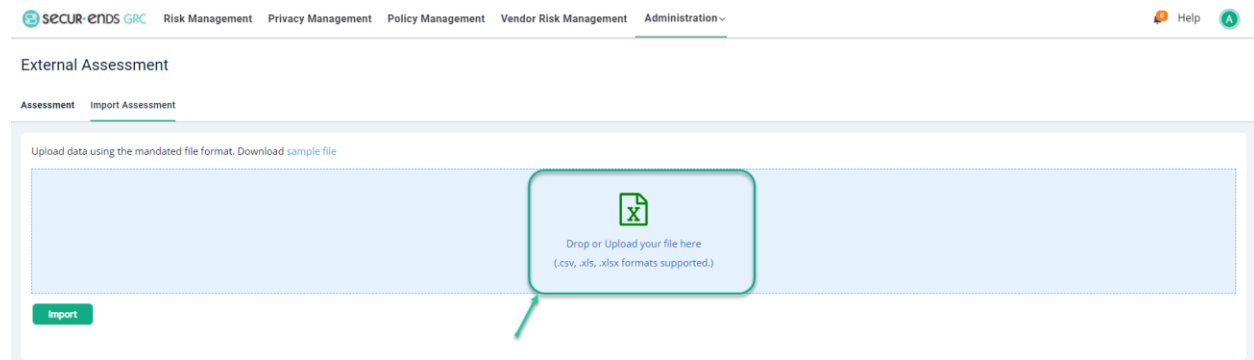
Click the **Administration** tab on the main menu and select **External Assessment** from the drop-down list.



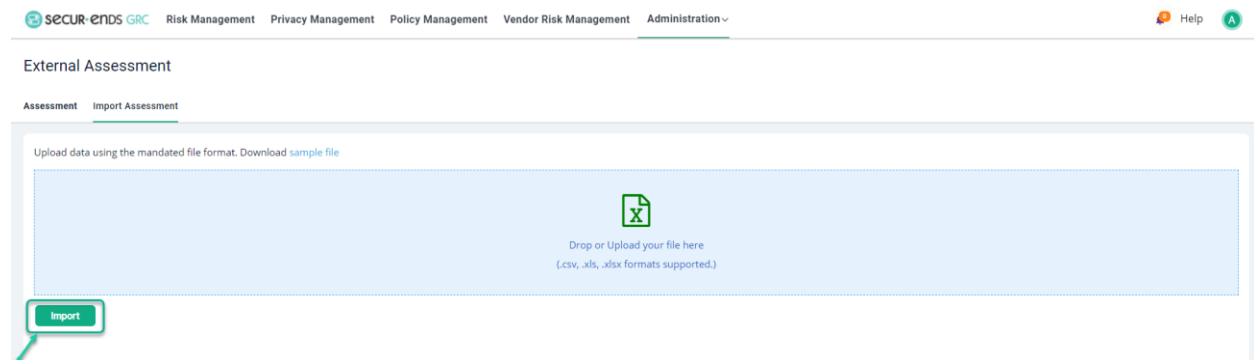
Click the **Import Assessment** button.



Drop or Upload Questionnaire file and click the **Import** button.



Click the **Import** button.

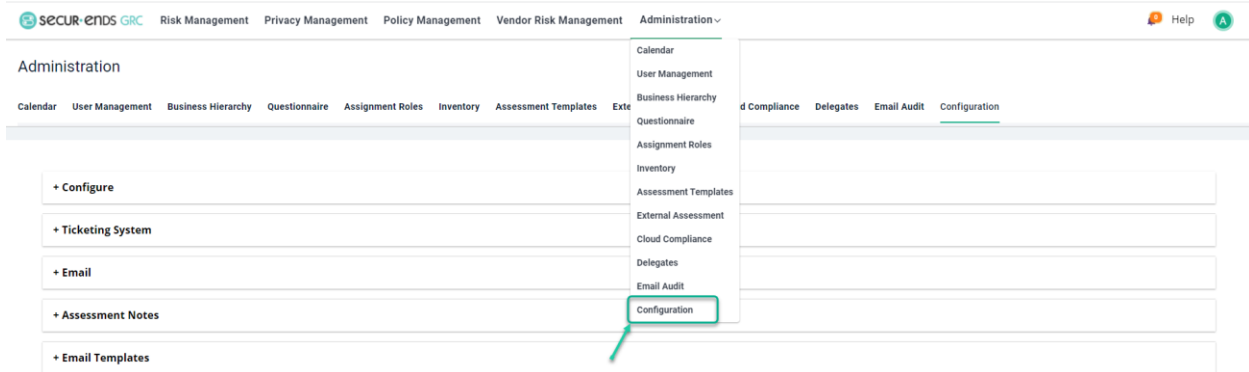


1.8 Configuration

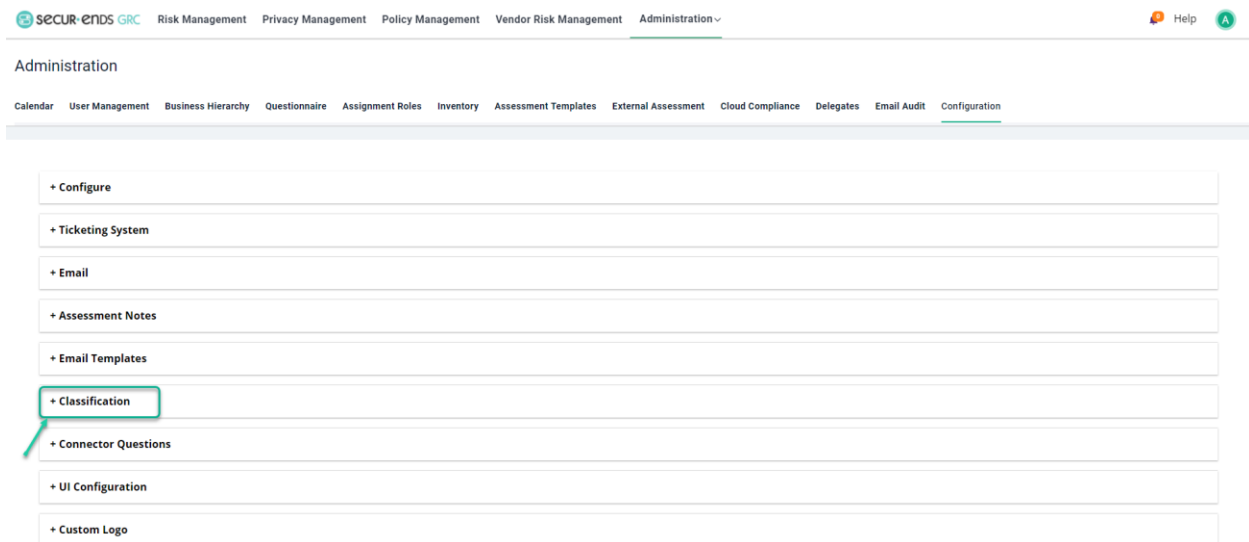
An assortment of options for system customization is available in the Configuration menu.

Classification

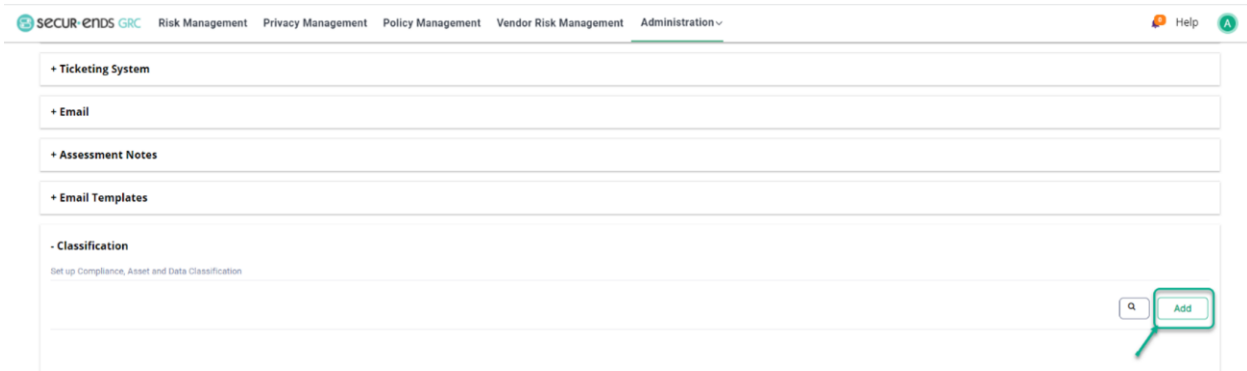
Select the **Configuration** option in **Administration** drop-down menu.



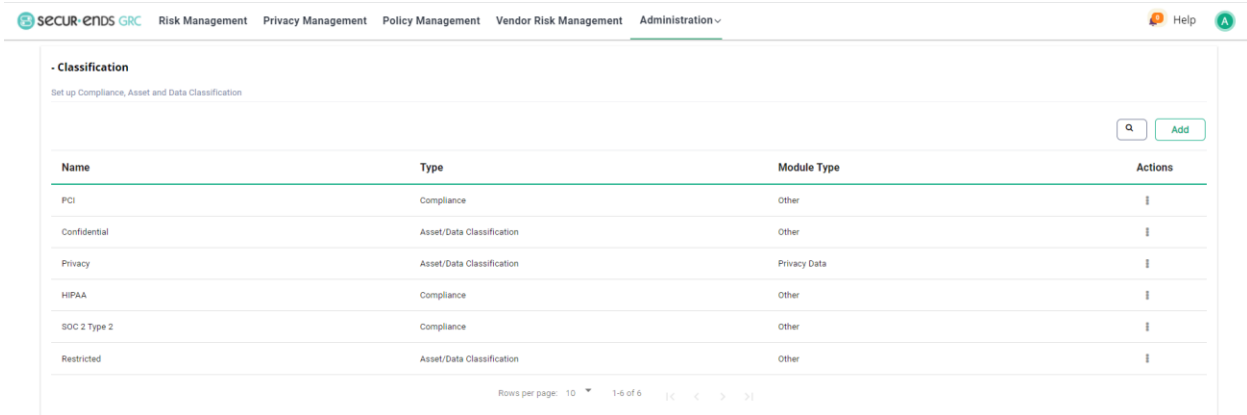
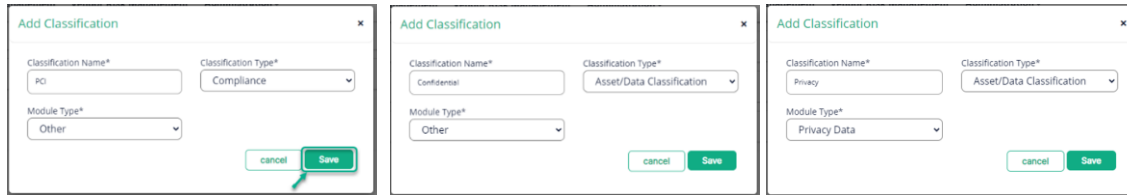
Select Classification.



Click the **Add** button to setup Compliance, Asset and Data Classification.



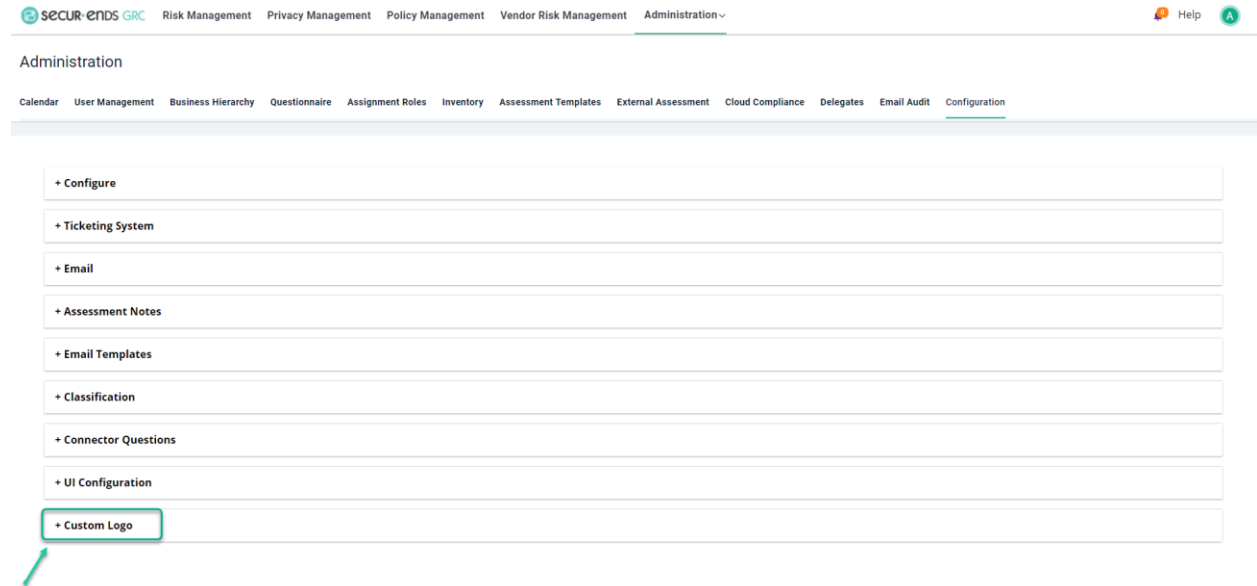
Enter **Classification Name** and Select **Classification Type** and **Module Type** in drop down list and click the **Save** button with these options.



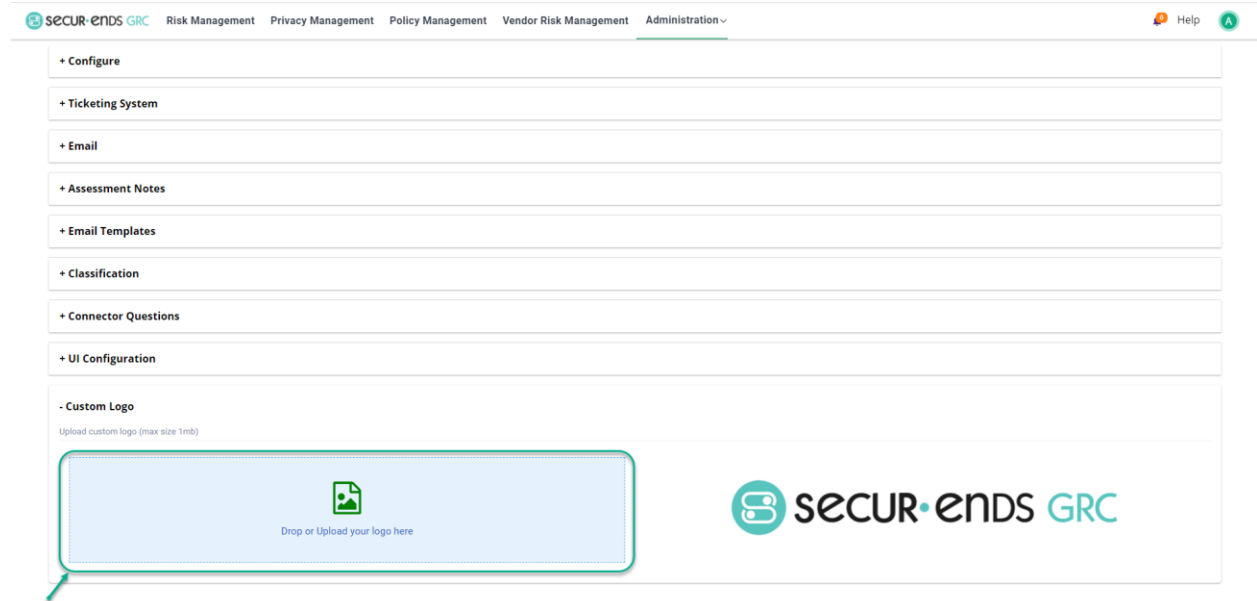
Custom Logo

Select the **Configuration** option in **Administration** drop-down menu.

Click the **Custom Logo** option.



Drop or Upload Logo.



[End of Administration User Guide]