



NIST Cybersecurity Framework Module

Step-by-Step Tutorial

Document Version: 02.00.03 | December 2018

Rsam © 2018. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

Contents

About Rsam Tutorials	3
Rsam Sandbox Environment.....	4
NCSF Assessment Framework	5
Overview	5
NCSF Workflows	5
NCSF Profile Assessment Workflow	6
Control Requirements Workflow	7
Action Plan Workflow.....	7
Tier Attestation Workflow	8
User Accounts	8
High-Level Steps	9
NCSF Profile Assessment	10
Step 1: Creating an NCSF Profile Assessment Object	10
Step 2: Starting an NCSF Profile Assessment	11
Step 3: Updating an NCSF Profile Assessment.....	13
Step 4: Reviewing and Approving NCSF Profile Assessment Details	15
Control Requirements	17
Step 1: Assessing a Control Requirement	18
Step 2: Submitting a Control Requirement.....	23
Step 3: Reviewing a Control Requirement	23
Tier Attestation	25
Step 1: Generating an Attestation Record	25
Step 2: Attesting to an NCSF Profile Assessment.....	25
Finalizing NCSF Assessments	28
NCSF Assessment Status Summary	29
Working with Assessment Status Summary	30
Generating a Report	30
NCSF Function and Category Details	31
Overall Summary of Assessments	31
Appendix 1: Creating Action Plans from Outside a Profile Assessment	32
Creating an Action Plan	32
Approving an Action Plan.....	33
Validating an Action Plan	34
Appendix 2: Rsam Documentation	35

About Rsam Tutorials

The Rsam module step-by-step tutorials are designed to help you learn about a specific Rsam module and to gain basic familiarity with the user interface. The Rsam platform is highly configurable and is capable of handling both simple and comprehensive applications. The step-by-step tutorials and Rsam sandboxes, however, are specifically designed to quickly deliver a user experience without requiring further training. Each step-by-step tutorial walks you through common, out-of-the-box functionality within a given Rsam module, allowing you to get immediate hands-on familiarity with the module.

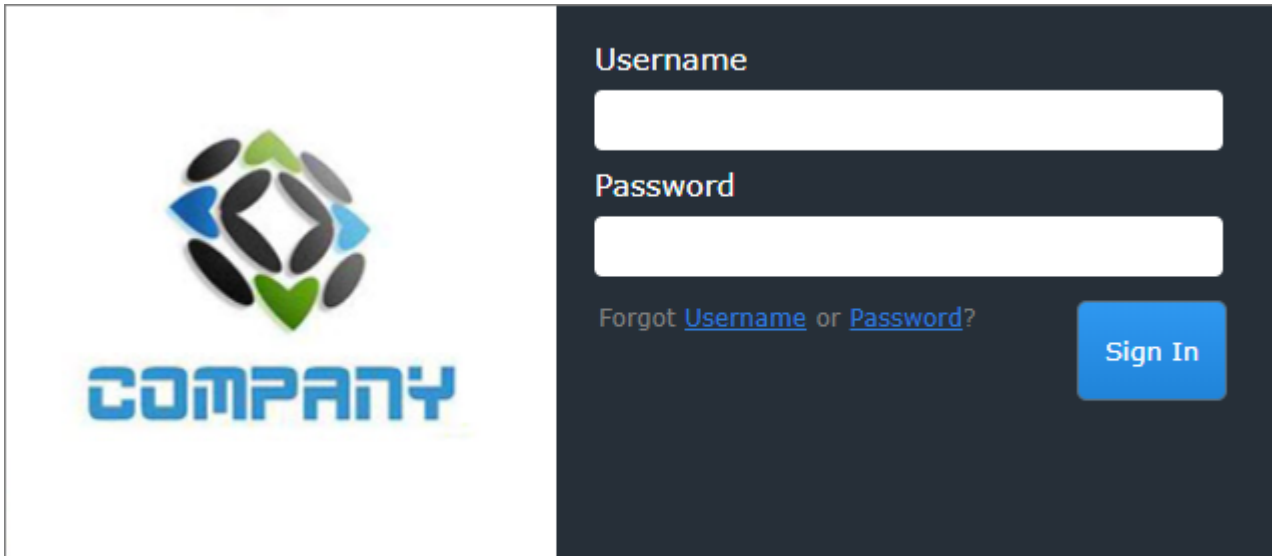
Rsam Sandbox Environment

Rsam module step-by-step tutorials are designed to work with the out-of-the-box Rsam configuration. You may follow this tutorial using an Rsam Sandbox environment or using your own instance of Rsam that you already own. If you are using this tutorial with an Rsam Sandbox environment, the URL to access your Rsam sandbox is delivered through an email. Otherwise, you may contact your Rsam Administrator for the URL to access your Rsam instance.

If you are using an Rsam sandbox environment, you should have provided Rsam with your organization’s internet facing IP address. To find this information, open a browser and connect to an IP discovery site such as www.whatismyip.com, or contact your organization’s Network Administrator for assistance. You may also contact your Rsam Customer Representative with any questions.

Sign-In Page

Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign-In page so that you can easily toggle between various sample accounts used throughout the tutorial.



Like most elements in Rsam, the Sign-In page can be configured in a number of ways. Different authentication options such as user self-registration, integration with customer user directories (such as Active Directory), or integration with Single Sign-On products, such as Shibboleth, can be applied. You can also embed your own branding and logo on the Sign-In page.

NCSF Assessment Framework

Overview

Rsam NIST Cybersecurity Assessment Framework (NCSF) module allows users to create, scope, and assess cybersecurity *profiles* as defined by the NIST Cybersecurity Framework. Users assess profiles against individual *subcategories* provided by the Cybersecurity Framework core utilizing the NIST concept of current and target *implementation tiers*. Users can then define action plans to address identified gaps, attest to the validity of assessments, and report over time on progress from the current state to the target state.

This tutorial covers the following phases of conducting a NIST Cybersecurity Assessment:

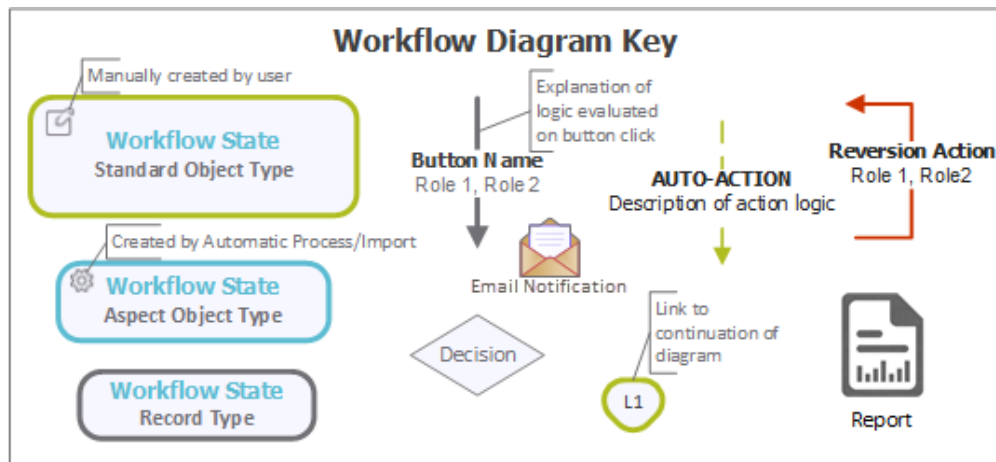
- [Creating and Scoping an NCSF Assessment Profile](#)
- [Assessing Control Requirements](#)
- [Developing Action Plans](#)
- [Attesting to an NCSF Assessment](#)
- [Finalizing an NCSF Assessment](#)
- [Viewing NCSF Assessment Status Summary Charts and Reports](#)

NCSF Workflows

The NCSF module provides automated workflows for each of the following components:

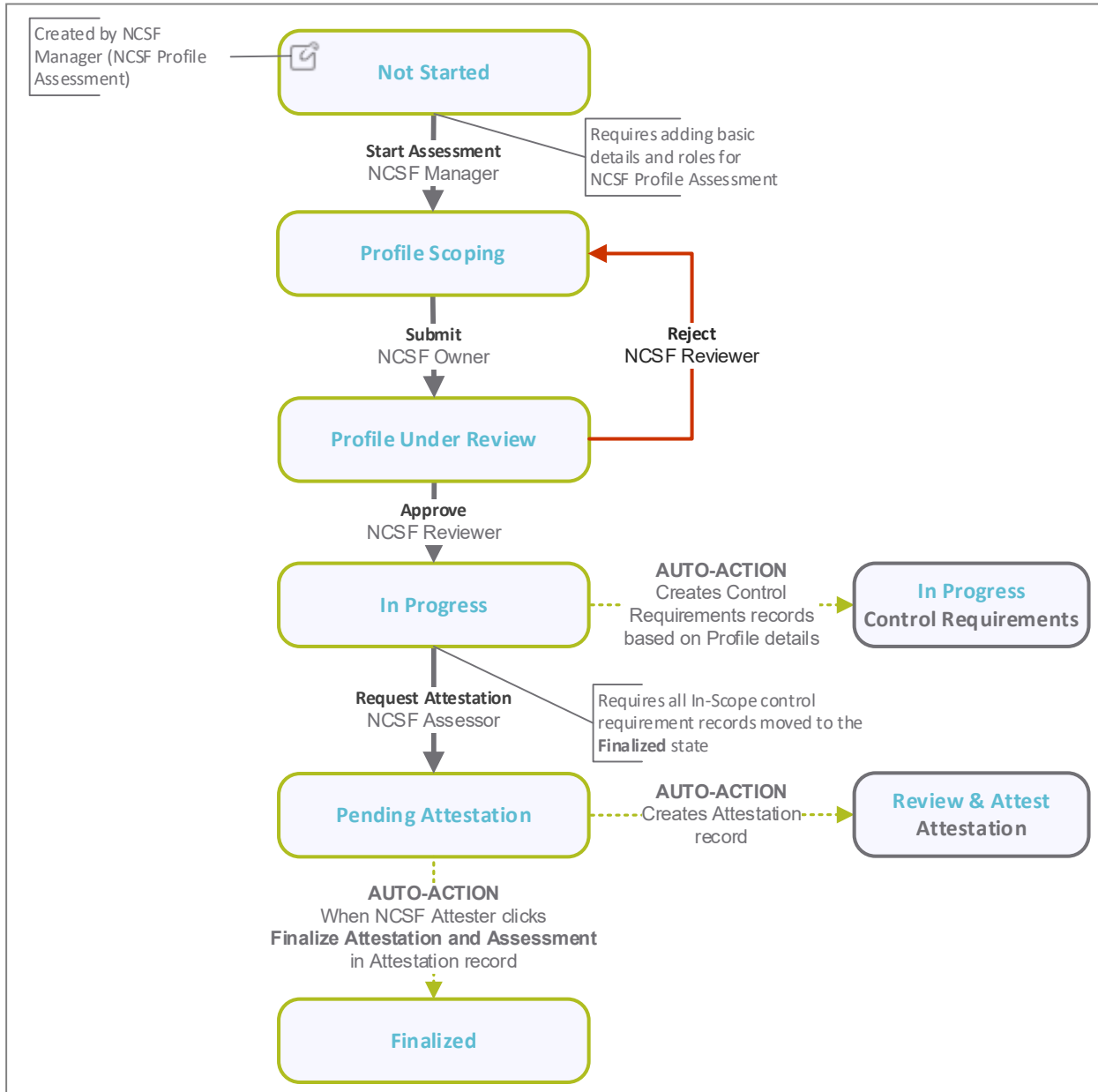
- [NCSF Profile Assessments](#)
- [Control Requirements](#) (assessments against each of the subcategories in the Framework core)
- [Action Plans](#)
- [Tier Attestations](#)

Before proceeding to the specific workflows, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.



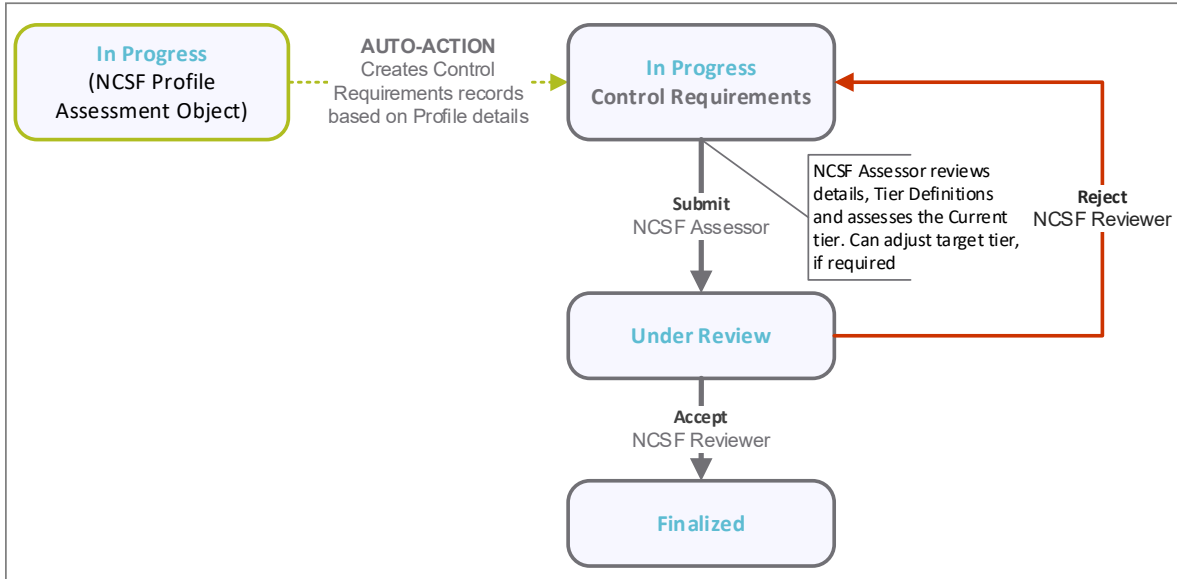
NCSF Profile Assessment Workflow

The following diagram shows the workflow of the NCSF Profile Assessment object.



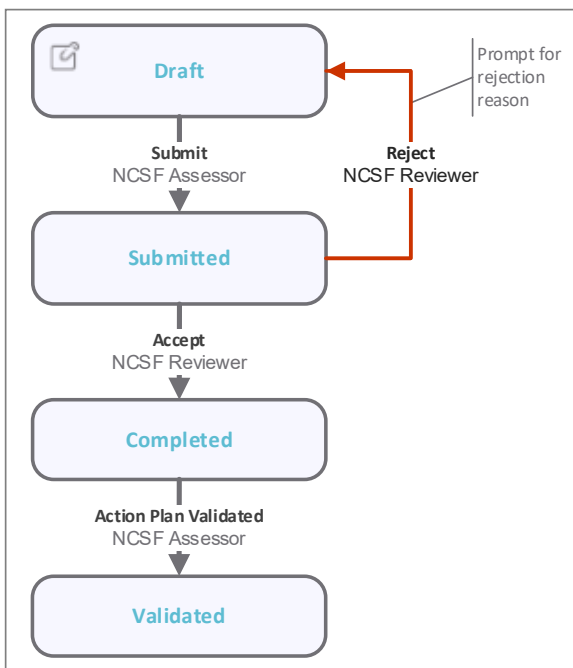
Control Requirements Workflow

The following diagram shows the workflow for each of the Control Requirement records, which reside within a NCSF Profile Assessment. Each Control Requirement record represents an assessment of a specific subcategory in the framework core.



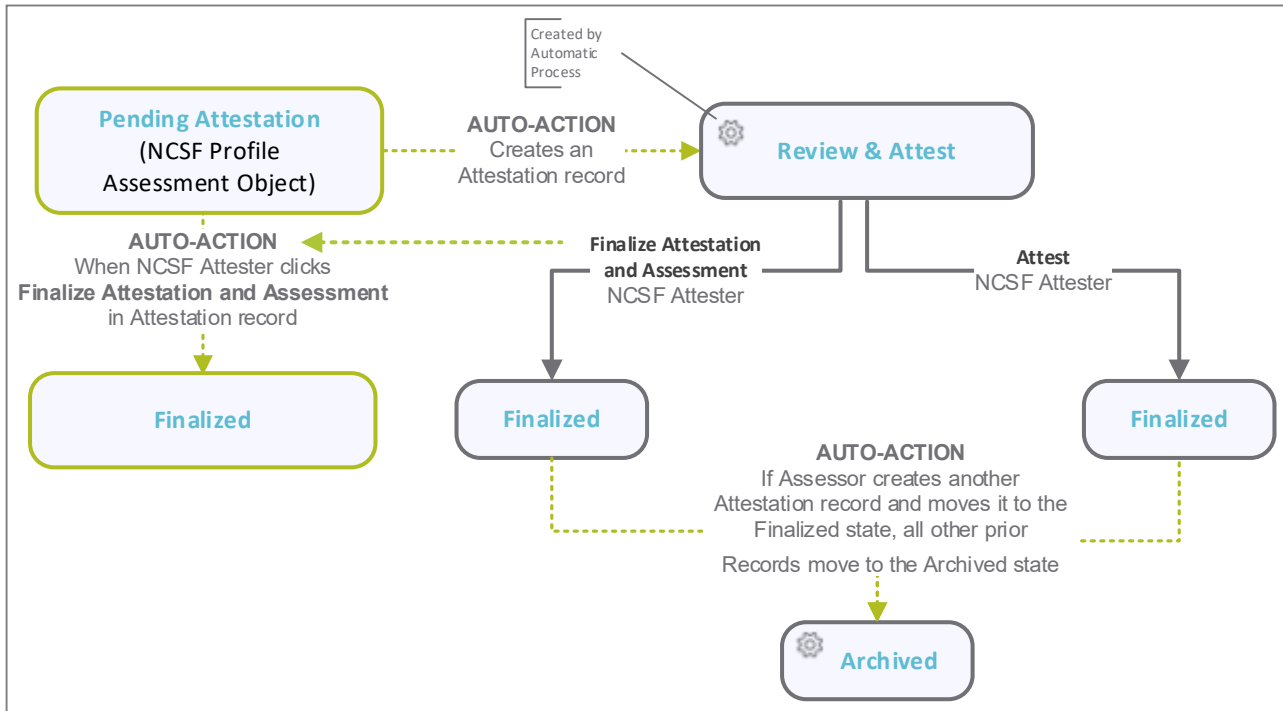
Action Plan Workflow

The following diagram shows the workflow for Action Plans configured to remediate gaps between current and target tiers.



Tier Attestation Workflow

The following diagram shows the workflow for the Tier Attestation records. These records help obtain periodic point-in-time sign-offs for respective NCSF Profile Assessments.



User Accounts

User accounts are required for the individuals authorized to access a specific Rsam baseline module. The Rsam sandbox for the NCSF Assessment Framework module comes with pre-populated sample accounts.

Note: Sample users for each of these roles are optionally provided with the baseline module installation package.

Account ID	User	Role Description
r_ncsf_manager	NCSF Manager	Has overall administrative access to all NCSF Profile Assessments and Control Requirements in the system. A user with this role is responsible for creating NCSF Profile Assessments and assigning the primary NCSF Owner and NCSF Assessor roles for assessments.
r_ncsf_owner	NCSF Owner	Responsible for defining and scoping the NCSF Profile Assessments to generate the required Control Requirements.
r_ncsf_reviewer	NCSF Reviewer	Responsible for reviewing NCSF Profile Assessments and related Control Requirements.
r_ncsf_assessor	NCSF Assessor	Responsible for assessing assigned Control

Account ID	User	Role Description
		Requirements.
r_ncsf_attester	NCSF Attester	Responsible for attesting to the entire NCSF Profile Assessment (including its individual control requirement assessments and action plans) prior to finalizing the assessment.

The default password for all accounts in the Rsam NCSF Assessment sandbox is *password*. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

High-Level Steps

The following is a high-level list of the steps described in this tutorial.

Step	User	Description
Step 1: Configuring Assessment Profile	NCSF Manager NCSF Owner NCSF Reviewer	Assessment profile is created, scope is defined, and moved to the In Progress state. In this state, Control Requirements are generated.
Step 2: Updating Control Requirements	NCSF Assessor NCSF Reviewer	Control Requirement records are assessed, action plans are associated, and reviewed and approved to progress to next state.
Step 3: Generating and Attesting Tiers	NCSF Assessor NCSF Attester	Attestation record is generated and the associated profile is attested.
Step 4: Finalizing Assessment Profile	Automatic process	Assessment Profile moves to Finalized state automatically when all the associated control requirements are reviewed and approved and are in the Finalized state.

NCSF Profile Assessment

An NCSF Profile Assessment contains details on how a given NCSF assessment is defined and scoped. It includes the following information:

- Subject of the assessment (lines of business, departments, etc.)
- Assigned roles and scheduled dates
- Related Asset-Level Assessments (for applications, vendors, etc.)
- NCSF Control Requirements (Subcategories) In-Scope

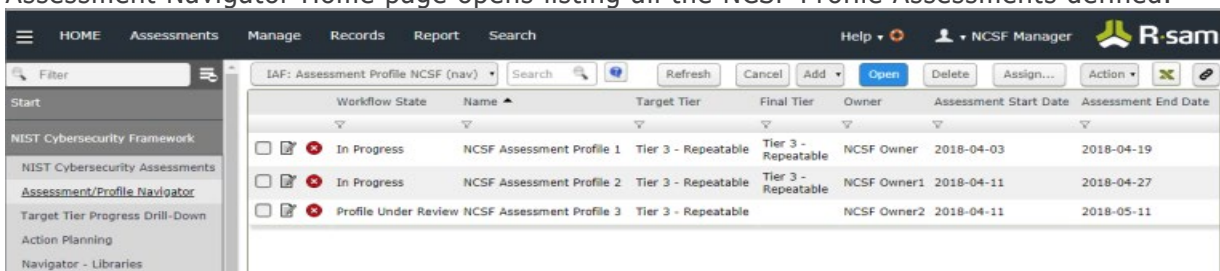
This chapter explains the following topics:

- [Step 1: Creating an NCSF Profile Assessment Object](#)
- [Step 2: Starting an NCSF Profile Assessment](#)
- [Step 3: Updating an NCSF Profile Assessment](#)
- [Step 4: Reviewing and Approving NCSF Profile Assessment Details](#)

Step 1: Creating an NCSF Profile Assessment Object

To create an NCSF Profile Assessment Object, perform the following steps:

1. Sign in to Rsam as the *NCSF Manager*. Provide the **Username** as *r_ncsf_manager* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator Home page opens listing all the NCSF Profile Assessments defined.



The screenshot shows the Rsam Assessment/Profile Navigator interface. The top navigation bar includes 'HOME', 'Assessments', 'Manage', 'Records', 'Report', and 'Search'. The user is logged in as 'NCSF Manager'. The main content area displays a table of NCSF Profile Assessments with columns for Workflow State, Name, Target Tier, Final Tier, Owner, Assessment Start Date, and Assessment End Date. The table contains three rows of data.

Workflow State	Name	Target Tier	Final Tier	Owner	Assessment Start Date	Assessment End Date
In Progress	NCSF Assessment Profile 1	Tier 3 - Repeatable	Tier 3 - Repeatable	NCSF Owner	2018-04-03	2018-04-19
In Progress	NCSF Assessment Profile 2	Tier 3 - Repeatable	Tier 3 - Repeatable	NCSF Owner1	2018-04-11	2018-04-27
Profile Under Review	NCSF Assessment Profile 3	Tier 3 - Repeatable		NCSF Owner2	2018-04-11	2018-05-11

3. On the right panel, select **Add > Object**. The **Create New Object** dialog appears.
 - a. Provide a name for the NCSF Profile Assessment, *TRN: Assessment Profile*, in the **Object Name** field.

- b. Select **Assessment Framework (NCSF)** from the drop down list available in the **Object Type** field.

Object Name:

Sub Entity:

Object Type:

- c. Click **Save** to save the object. The dialog closes.

The created object appears on the Assessment Navigator list, in the **Not Started** state.

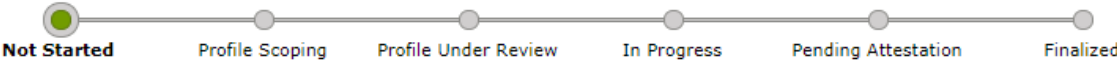
Step 2: Starting an NCSF Profile Assessment

After creating an NCSF Profile Assessment Object, the NCSF Manager must start the assessment by assigning roles and setting the assessment schedule. To start an assessment, perform the following steps:

1. Stay signed in as the *NCSF Manager*.
2. On the Assessment Navigator page, double-click the NCSF Profile Assessment Object to open it. The Details page opens listing details of the NCSF Profile Assessment.

Assessment Framework (NCSF): TRN: Assessment Profile

Workflow State: Not Started	Name: TRN: Assessment Profile
Target Tier:	Final Tier:
Owner:	Assessment Start Date:
Assessment End Date:	



Not Started Profile Scoping Profile Under Review In Progress Pending Attestation Finalized

Cybersecurity Profile

Name	Questionnaire	State			
TRN: Assessment Profile	0 of 1 answered	Not Started			


Cybersecurity Core

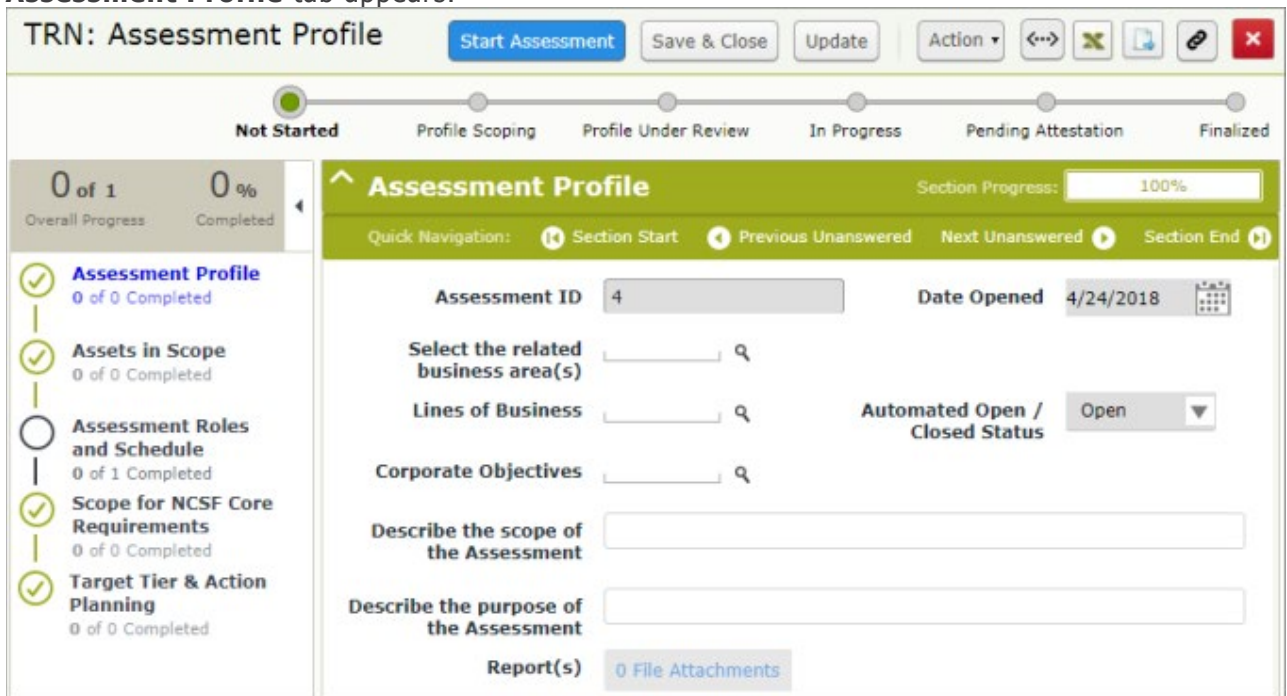
[Control Requirements \(0\)](#)

[Attestations \(0\)](#)

[IAF Indicators \(0\)](#)

<p>In-Scope Control Requirement Assessment Progress</p> <p>No Data Found for this Component for this object</p>	<p>In-Scope Control Requirements by NCSF Function</p> <p>No Data Found for this Component for this object</p>
---	---

- Click  corresponding to the Object name to open the NCSF Profile Assessment. The **Assessment Profile** tab appears.



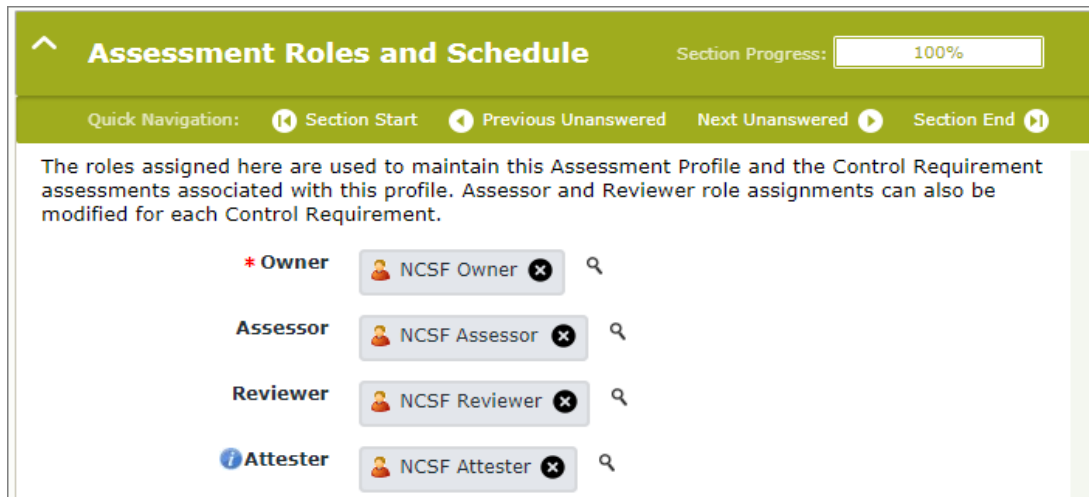
Values in the **Assessment ID**, **Date Opened**, **Automated Open / Closed Status** fields are auto-populated.

- Provide values for any of the desired, optional fields in the **Assessment Profile** tab.
- Click **Assessment Roles and Schedule** tab and perform the following:
 - Provide values for the roles, as mentioned in the following table.

Field	User Role
Owner	<i>NCSF Owner</i>
Assessor	<i>NCSF Assessor</i>
Reviewer	<i>NCSF Reviewer</i>
Attester	<i>NCSF Attester</i>

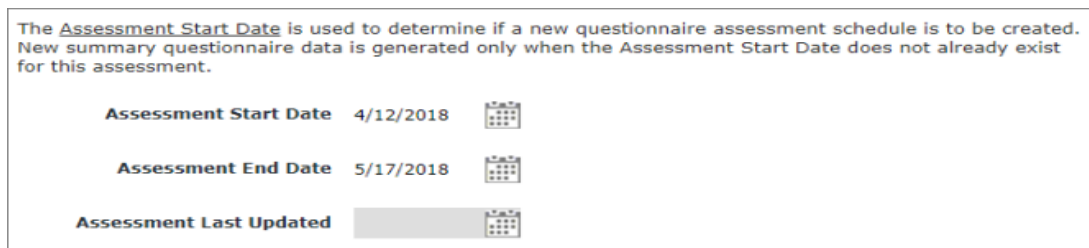
Owner is the only role that is required to be set to start the Assessment but the user can set values for all other roles as these are required at the next stages as the profile progresses.

The following image shows the **Assessment Roles and Schedule** tab.



b. Provide values for the following:

- **Assessment Start Date** - Date when the assessment must be started.
- **Assessment End Date** - Date by when the assessment must be finished.




6. Validate the values provided and click **Start Assessment**. The responses are saved and the NCSF Profile Assessment moves to the **Profile Scoping** state. The page refreshes to show the Object Details.

Step 3: Updating an NCSF Profile Assessment

The NCSF Owner must now provide further information to define and scope the profile assessment. Specifically, the NCSF Owner determines which subcategories of the NIST Cybersecurity Framework core are *in scope*, whether and how to set default values for *target tiers*, and whether to require action plans for identified gaps. These details are then submitted to the NCSF Reviewer for review.

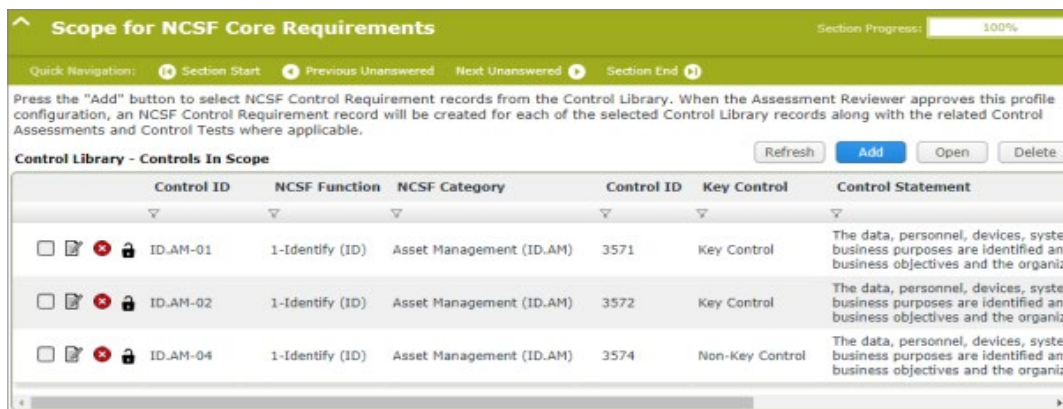
Note: In this stage of the workflow, an Assessment Profile can also be mapped to specific *Assets in scope* so that the questionnaire results identified in the Asset-level Assessments will be displayed in the related Control Requirements to inform current and target tier assessments for those requirements. However, while the NCSF Assessment Framework Module is designed to integrate data from the asset-level Risk & Compliance Assessments Module, the Risk & Compliance Assessments Module is licensed separately and the steps are not covered in this tutorial.

To provide the scope and Asset details, perform the following steps:

1. Sign in to Rsam as the *NCSF Owner*. Provide the **Username** as *r_ncsf_owner* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator page opens listing the NCSF Profile Assessments applicable for your role.
3. On the **Assessment Navigator** page, double-click an Object in the **Profile Scoping** state to open it. The Details page opens listing details of the NCSF Profile Assessment.
4. Click  corresponding to the NCSF Profile Assessment Object to open the Assessment Profile.
5. In this step you will determine which specific subcategories from the NIST Cybersecurity Framework core to include in the scope of this profile assessment. Click **Scope for NCSF Core Requirements** tab to add the control requirements in scope for the profile.
 - a. Click **Add**. The **Control Library - Controls In Scope** dialog appears.
 - b. Select the first three controls from the **Identify** function and click **Update**. The selected controls are added to the list.

Note: For the purpose of completing the baseline configuration following this tutorial, selecting three or lesser number of controls ensure that you can quickly advance all the control requirements to the final state before sending for attestation and finalization of the profile. However, when configuring an actual customer scenario, you can select all the required functions and controls.

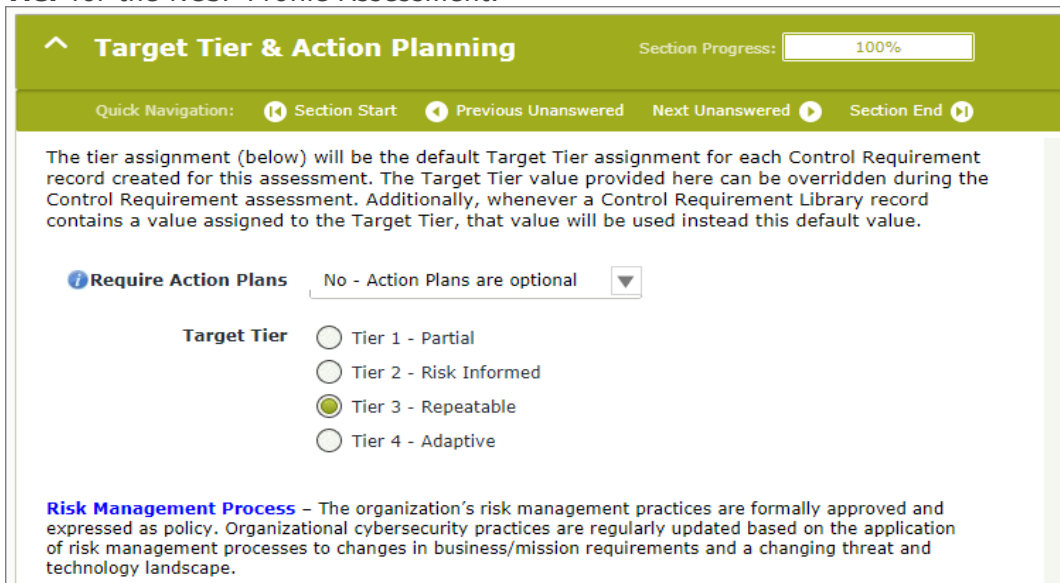
The following image shows the controls added to the **Scope for NCSF Core Requirements** tab.



The screenshot shows a dialog box titled "Scope for NCSF Core Requirements" with a "Section Progress" indicator at 100%. Below the title bar, there are navigation buttons: "Section Start", "Previous Unanswered", "Next Unanswered", and "Section End". A text box explains that clicking "Add" will create NCSF Control Requirement records. Below this, there are buttons for "Refresh", "Add", "Open", and "Delete". The main content is a table titled "Control Library - Controls In Scope" with the following data:

Control ID	NCSF Function	NCSF Category	Control ID	Key Control	Control Statement
<input type="checkbox"/> ID.AM-01	1-Identify (ID)	Asset Management (ID.AM)	3571	Key Control	The data, personnel, devices, system business purposes are identified and business objectives and the organization's
<input type="checkbox"/> ID.AM-02	1-Identify (ID)	Asset Management (ID.AM)	3572	Key Control	The data, personnel, devices, system business purposes are identified and business objectives and the organization's
<input type="checkbox"/> ID.AM-04	1-Identify (ID)	Asset Management (ID.AM)	3574	Non-Key Control	The data, personnel, devices, system business purposes are identified and business objectives and the organization's

6. In this step you will determine how Rsam sets default values for *target tiers* and whether Rsam will require action plans for identified gaps. Click **Target Tier & Action Planning** tab and perform the following:
 - a. The **Require Action Plans** field determines whether Rsam will require actions plans to be created for Control Requirements that have gaps between their current and target tier designations. Select **No – Action Plans are optional**.
 - b. The **Target Tier** field will default the target tier for the individual Control Requirements that will be generated later it the workflow. Select any value (or no value) as the **Target Tier** for the NCSF Profile Assessment.



Target Tier & Action Planning Section Progress: 100%

Quick Navigation: Section Start Previous Unanswered Next Unanswered Section End

The tier assignment (below) will be the default Target Tier assignment for each Control Requirement record created for this assessment. The Target Tier value provided here can be overridden during the Control Requirement assessment. Additionally, whenever a Control Requirement Library record contains a value assigned to the Target Tier, that value will be used instead this default value.

Require Action Plans No - Action Plans are optional

Target Tier

- Tier 1 - Partial
- Tier 2 - Risk Informed
- Tier 3 - Repeatable
- Tier 4 - Adaptive

Risk Management Process – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

Note: If target tier values are provided for the individual Control Requirements in the Control Library, the target tier provided here will be overridden. The management of Library Controls is not covered in this document.

7. Click **Submit** to submit the profile for review. The profile moves to the **Profile Under Review** state.

Step 4: Reviewing and Approving NCSF Profile Assessment Details

An NCSF Reviewer must review the profile details provided by the NCSF Owner and approve or reject the details. To review and approve the details, perform the following steps:

1. Sign in to Rsam as the *NCSF Reviewer*. Provide the **Username** as *r_ncsf_reviewer* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator page opens listing the assigned assessment profiles.

3. On the **Assessment Navigator** page, double-click an Assessment Object in the **Profile Under Review** state to open it. The Details page opens listing details of the Assessment Object.
4. Click to open the Assessment Profile.
5. Review the details provided in the different tabs of the NCSF Profile Assessment.
6. Click **Approve** to approve the NCSF Profile Assessment details. A confirmation dialog appears stating that continuing the action will move the profile to the **In Progress** state and create Control Requirement records, based on the criteria.
7. Click **OK** in the confirmation dialog that appears. The profile moves to the **In Progress** state and Control Requirements are automatically generated for the NCSF Profile Assessment, based on the defined scope. The generated Control Requirement records are specific to this NCSF Profile Assessment and serve as the work spaces where control-level tier assessments will be managed and tracked.

Assessment Framework (NCSF): TRN: Assessment Profile

Workflow State: In Progress	Name: TRN: Assessment Profile
Target Tier: Tier 3 - Repeatable	Final Tier:
Owner: NCSF Owner	Assessment Start Date:
Assessment End Date:	

Not Started Profile Scoping Profile Under Review **In Progress** Pending Attestation Finalized

Cybersecurity Profile

Name	Questionnaire	State			
TRN: Assessment Profile	1 of 1 answered	In Progress			

Cybersecurity Core

[Control Requirements \(3\)](#)
[Attestations \(0\)](#)

In-Scope Control Requirement Assessment Progress

In-Scope Control Requirements by NCSF Function

	3
1-Identify (ID)	

No Data

Note: Now, users with the assigned roles can navigate to the control requirement records, update and submit the requirements for review.

Control Requirements

Control Requirement records track the individual workflows for assessing the current and target tiers for specific Control Requirements determined to be in scope for an NCSF Profile Assessment. Control Requirements for each NCSF Profile Assessment are generated when the NCSF Reviewer approves the profile. These individual requirement records can then be populated with details and progressed to the further states.

This chapter explains the following topics:

- [Step 1: Assessing a Control Requirement](#)
 - o [Step 1a: Creating an Action Plan](#)
 - o [Step 1b: Approving an Action Plan](#)
 - o [Step 1c: validating an Action Plan](#)
- [Step 2: Submitting a Control Requirement](#)
- [Step 3: Reviewing a Control Requirement](#)

Note: This tutorial assumes that the NCSF Assessor has all information available that is required to make informed decisions about the current tier designation, target tier designation, and any required action plans for the subcategory. However, Rsam NCSF module is designed with out-of-the-box integrations with other Rsam modules to display relevant information that supports data-driven decisions. Rsam NCSF module integrates specifically with the following modules, each of which is licensed separately:

- **Rsam Risk and Compliance Assessments module:** If customers are using Rsam Risk and Compliance Assessments module, the relevant results of any asset-level, survey-based assessments associated with the NIST Cybersecurity profile assessment will be visible on the **Questionnaire Results** tab of each Control Requirement. For survey-based assessment data to appear within a Control Requirement record, customers must ensure the following requirements are met:
 - o Rsam Risk and Compliance Assessments module is deployed in their Rsam environment.
 - o Specific asset objects (IT applications, vendors, etc.) are associated with the NIST Cybersecurity Profile Assessment object during the scoping phase.
 - o Survey-based assessments have been conducted against those assets using Assessment Questions that have been mapped to the NIST Cybersecurity Framework control library. Rsam-harmonized Assessment Questions and Rsam NIST 800-53 assessment questions have been pre-mapped to the NCSF control library, so customers that have licensed either of these content packs from Rsam do not need to establish those mappings themselves.For more information on the Risk and Compliance Assessments module, refer the *Risk and Assessment Step-by-Step Tutorial*.

- **Rsam Continuous Controls Testing module:** The NCSF module includes one pre-defined control test for each subcategory in the Framework core. To leverage these supplied control tests (or customer-defined tests) to support tier designations, customers must license the Continuous Controls Testing module. For more information on the Continuous Controls Testing module, refer the *Continuous Controls Testing Step-by-Step Tutorial*.
- **Rsam Indicators module:** The Indicators module allows customers to define indicators for any additional data that might support decisions around NIST Cybersecurity implementation tier designations. Indicator data can be sourced manually from users, automatically from the results of saved searches executed against other Rsam modules, or from data that has been integrated from other tools (for example, vulnerability scanners). For more information on the Indicators module, refer the *Indicators Step-by-Step Tutorial*.

Step 1: Assessing a Control Requirement

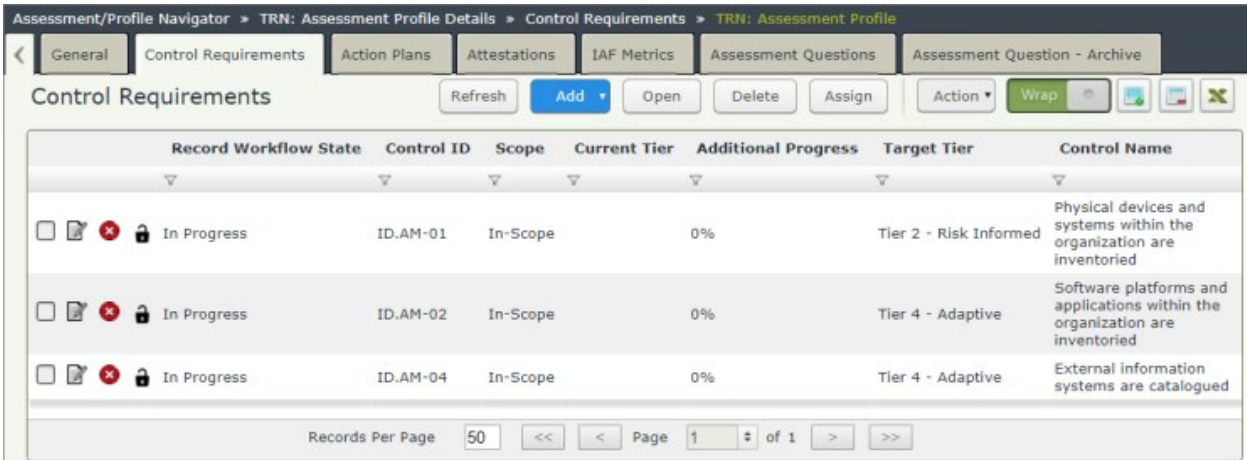
In this step of the workflow, the NCSF Assessor will specify the current and target implementation tiers for the Control Requirement. Additionally, if the current tier does not meet the target, the assessor may be required to enter one or more Action Plans to address the identified gap.

Note: Assessors can be assigned to individual Control Requirements or can be assigned at the NCSF Profile Assessment level. In our case, we have assigned NCSF Assessor user at the profile level, so there is no need to assign specific assessors for each Control Requirement.

To assess a control requirement, perform the following steps:

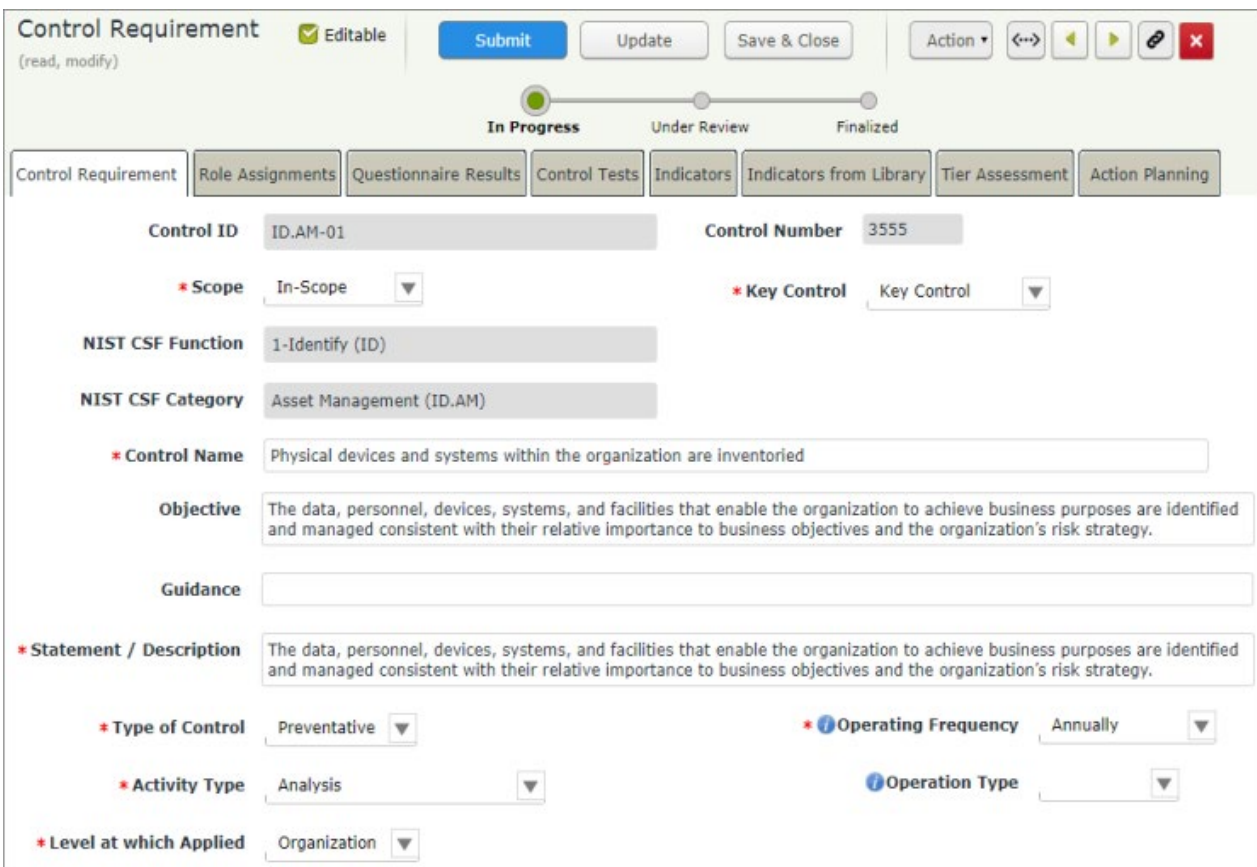
1. Sign in to Rsam as the *NCSF Assessor*. Provide the **Username** as *r_ncsf_assessor* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator page opens.
3. On the **Assessment Navigator** page, double-click the assigned NCSF Profile Assessment Object to open it. The Details page opens listing details of the NCSF Profile Assessment.
4. Click the **Control Requirements (x)** link to open the Control Requirements generated for the profile assessment.

The **Control Requirements** page opens listing all the applicable Control Requirements.



Record Workflow State	Control ID	Scope	Current Tier	Additional Progress	Target Tier	Control Name
In Progress	ID.AM-01	In-Scope		0%	Tier 2 - Risk Informed	Physical devices and systems within the organization are inventoried
In Progress	ID.AM-02	In-Scope		0%	Tier 4 - Adaptive	Software platforms and applications within the organization are inventoried
In Progress	ID.AM-04	In-Scope		0%	Tier 4 - Adaptive	External information systems are catalogued

- Double-click the first Control Requirement record to open it. The record opens with the **Control Requirement** tab selected.



Control Requirement (read, modify) Editable

Submit Update Save & Close Action

In Progress Under Review Finalized

Control Requirement Role Assignments Questionnaire Results Control Tests Indicators Indicators from Library Tier Assessment Action Planning

Control ID: ID.AM-01 Control Number: 3555

* Scope: In-Scope * Key Control: Key Control

NIST CSF Function: 1-Identify (ID)

NIST CSF Category: Asset Management (ID.AM)

* Control Name: Physical devices and systems within the organization are inventoried

Objective: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Guidance:

* Statement / Description: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

* Type of Control: Preventative * Operating Frequency: Annually

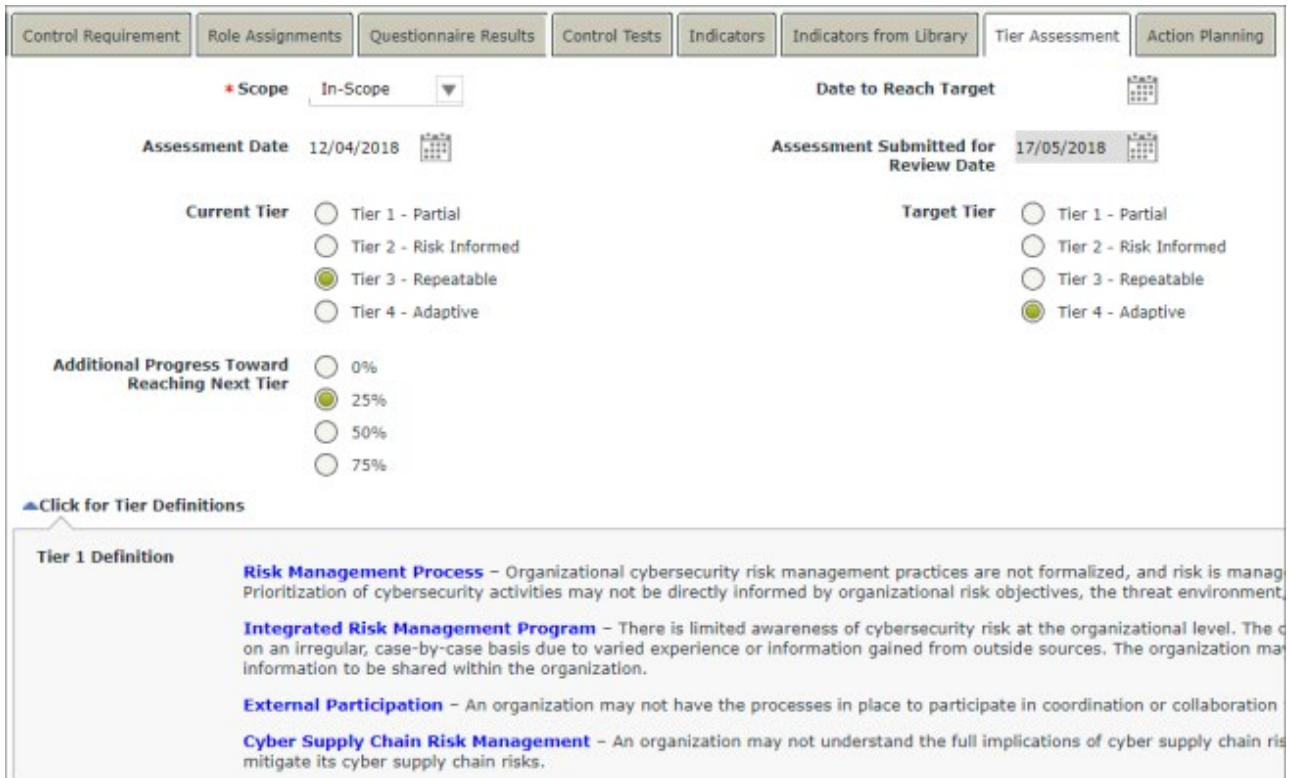
* Activity Type: Analysis * Operation Type:

* Level at which Applied: Organization

The Control Requirement tab displays general information about the subcategory as defined in the NCSF core.

6. Review the information in the Control Requirement tab to get an understanding of the requirement you are assessing.
7. Click the **Tier Assessment** tab. The tab displays attributes for capturing the current tier, target tier, and other information relevant to the tier assessments.

Before providing any values in this tab, click the expand icon next to the **Click for Tier Definitions** attribute to display explanations of each of the tiers.



The screenshot displays the 'Tier Assessment' tab with the following configuration:

- Scope:** In-Scope
- Assessment Date:** 12/04/2018
- Date to Reach Target:** (Calendar icon)
- Assessment Submitted for Review Date:** 17/05/2018
- Current Tier:**
 - Tier 1 - Partial
 - Tier 2 - Risk Informed
 - Tier 3 - Repeatable
 - Tier 4 - Adaptive
- Target Tier:**
 - Tier 1 - Partial
 - Tier 2 - Risk Informed
 - Tier 3 - Repeatable
 - Tier 4 - Adaptive
- Additional Progress Toward Reaching Next Tier:**
 - 0%
 - 25%
 - 50%
 - 75%

Click for Tier Definitions

Tier 1 Definition

- Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have the processes in place to prioritize cybersecurity activities or to share information to be shared within the organization.
- Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level. The organization may not have the processes in place to participate in coordination or collaboration with external organizations to mitigate its cyber supply chain risks.
- External Participation** – An organization may not have the processes in place to participate in coordination or collaboration with external organizations to mitigate its cyber supply chain risks.
- Cyber Supply Chain Risk Management** – An organization may not understand the full implications of cyber supply chain risks.

Note: These definitions are inherited from the library controls that represent the Framework core. The out-of-the-box definitions are taken directly from the NIST Cybersecurity Framework, but customers can optionally configure them to match their own tier definitions.

- a. Select **Tier 4 - Adaptive** for the **Target Tier** field.

Note: The Target Tier value may be pre-selected with a different value specified either within the control library or during the scoping for this profile assessment. If so, overwrite the default value by selecting **Tier 4 – Adaptive** to complete this tutorial.

- b. Select **Tier 3 - Repeatable** for the **Current Tier** field.

Note: For this tutorial, we are selecting a lower value than the Target Tier so that you can explore the creation of an Action Plan to address this gap.

- c. Select a value in the **Additional Progress Toward Reaching Next Tier** field. While the NCSF Control Requirements are assessed primarily using the four-valued tier designations, the module allows for more granular tracking of current progress from the current tier to the next tier. The value specified for this field provides for more granular assessment of the current tier and is reflected in reports such as the [Target Tier Progress Drill-Down report](#).
- d. Provide the **Date to Reach Target** for the control requirement.

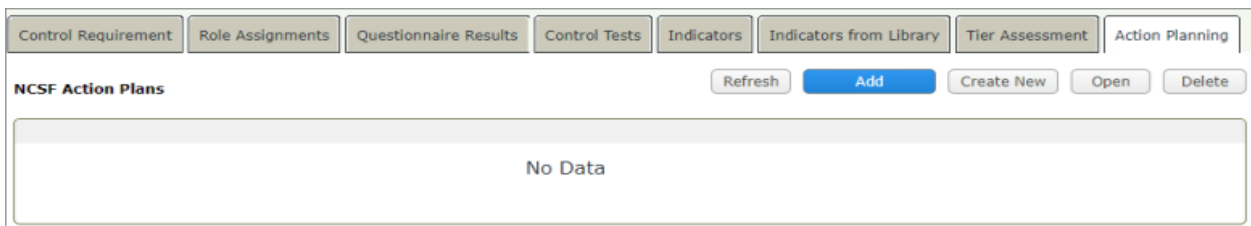
Step 1a: Creating an Action Plan

In this tutorial workflow, since the Current Tier is set to a lower value than the Target Tier, we will create an Action Plan to address this gap. Click the **Action Planning** tab in the Control Requirement record to add an action plan.

Note: If you prefer to skip adding action plans, the appropriate selection must have been done for the [Require Action Plans](#) field when setting up the Profile Assessment in previous steps.

You can either create new action plans or associate already existing plans. In this tutorial, we will create a new action plan:

1. Stay signed in as the *NCSF Assessor* and click **Create New** button that appears above the **NCSF Action Plans** section.



2. Provide values in the required fields and click **Submit** to submit the action plan.
3. Click **OK** in the confirmation dialog that appears.
4. Click **Save & Close** to close the Control Requirement record.

Step 1b: Approving an Action Plan

An action plan must be reviewed and approved before the Profile Assessment can be finalized. To approve an action plan, perform the following steps:

1. Sign in to Rsam as the *NCSF Reviewer*. Provide the **Username** as *r_ncsf_reviewer* and **Password** as *password*.

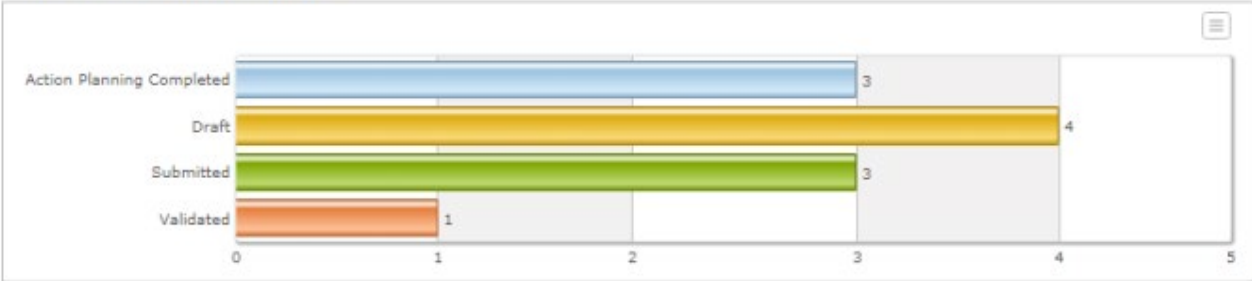
- Navigate to **NIST Cybersecurity Framework > Action Planning**. A page appears listing details of all Action Plans in the system.

Action Plans

Search Refresh Cancel Add Open Delete Assign... Action Go to

Workflow State	Name	Action Plan Title	Date Opened
Action Planning Completed	GDPR Assessment 1	General GDPR Action Plan	2018-04-11
Draft	Global Action Plan	Global Action Plan from GDPR Article 44	2018-04-04
Draft	Global Action Plan	Global Action Plan from GDPR Article 5	2018-04-04
Action Planning Completed	Global Action Plan	Global Action Plan from NCSF DE.AE.01	2018-04-04
Draft	Global Action Plan	Global Action Plan from NCSF DE.AE.02	2018-04-04
Submitted	Global Action Plan	Global Plan 5 for GDPR	2018-04-12
Draft	Global Action Plan	Global Plan 6 - GDPR	2018-04-12
Action Planning Completed	GDPR Assessment 2	Local Action Plan 1 - Article 6	2018-04-12
Submitted	GDPR Assessment 2	Local Action Plan 2 - Article 6	2018-04-12

Action Plans by Workflow State



Workflow State	Count
Action Planning Completed	3
Draft	4
Submitted	3
Validated	1

- Select the required action plan, review the details, and click **Accept**.
- Click **OK** in the confirmation dialog that appears. The action plan moves to the **Completed** state.

Step 1c: Validating an Action Plan

After an Action Plan has been approved, an Assessor must validate the plan. To validate an Action Plan, perform the following steps:

- Sign in to Rsam as the *NCSF Assessor*. Provide the **Username** as *r_ncsf_assessor* and **Password** as *password*.
- Navigate to **NIST Cybersecurity Framework > Action Planning**. A page appears listing details of all Action Plans in the system.

3. Select the required Action Plan in the **Completed** state and select **Action > Action Plan Validated**. The plan is validated and moves to the **Validated** state.

Step 2: Submitting a Control Requirement

After completing the action plan workflow, you can return to the Control Requirement and submit it for review. To submit a Control Requirement for review, perform the following steps:

1. Sign in to Rsam as the *NCSF Assessor*. Provide the **Username** as *r_ncsf_assessor* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator page opens.
3. On the **Assessment Navigator** page, double-click the assigned NCSF Profile Assessment Object to open it. The Details page opens listing details of the NCSF Profile Assessment.
4. Click the **Control Requirements (x)** link to view the Control Requirements generated for the profile assessment.
The **Control Requirements** page opens listing all the applicable Control Requirements.
5. Double-click the Control Requirement from the previous steps to open it. The record opens with the **Control Requirement** tab selected.
6. Click **Submit** to submit the control requirement, including the specified tier designations and action plans, for review.
A confirmation message appears stating that the control requirement is being submitted for review.
7. Click **OK** in the confirmation message dialog box. The responses are saved and the control requirement moves to the **Under Review** state.

Step 3: Reviewing a Control Requirement

An assigned NCSF Reviewer receives a notification when a control requirement is moved to the **Under Review** state. The reviewer must review the assessment details and Accept or Reject it. To review a control requirement, perform the following steps:

1. Sign in to Rsam as the *NCSF Reviewer*. Provide the **Username** as *r_ncsf_reviewer* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator page opens.

3. On the **Assessment Navigator** page, double-click the assigned NCSF Profile Assessment Object to open it. The Details page opens listing details of the NCSF Profile Assessment.
4. Click the **Control Requirements (x)** link to view the Control Requirements generated for the profile assessment.
The **Control Requirements** page opens listing all the applicable records.
5. Double-click the required Control Requirement, in the **Under Review** state, to open it. The record opens with the **Control Requirement** tab selected.
6. Validate all details provided.
7. Click **Accept** to accept the control requirement. The control requirement moves to the **Finalized** state.
8. Repeat the above steps for updating, submitting, and approving all the control requirements before continuing to the next section to request attestations of the profile. Attestations cannot be requested until all In-Scope Control Requirements are moved to the Finalized state.

Note: When accepting the last In-Scope control requirement record, a pop-up appears stating that all control requirements for the Profile are completed and users can continue with **Attestation** to finalize the assessment profile.

Tier Attestation

Before an NCSF Profile Assessment can be finalized, an NCSF Attester is responsible for reviewing the final tier assignment for the NCSF Profile Assessment and its related Control Requirements and attesting to the designated tier assignments.


This chapter explains the following topics:

- [Step 1: Generating an Attestation Record](#)
- [Step 2: Attesting to an NCSF Profile Assessment](#)

Note: Before requesting an attestation, all Control Requirements must be in the **Finalized** state, and any related action plans must be in the **Approved** state.

Step 1: Generating an Attestation Record

To generate an Attestation record, perform the following steps:

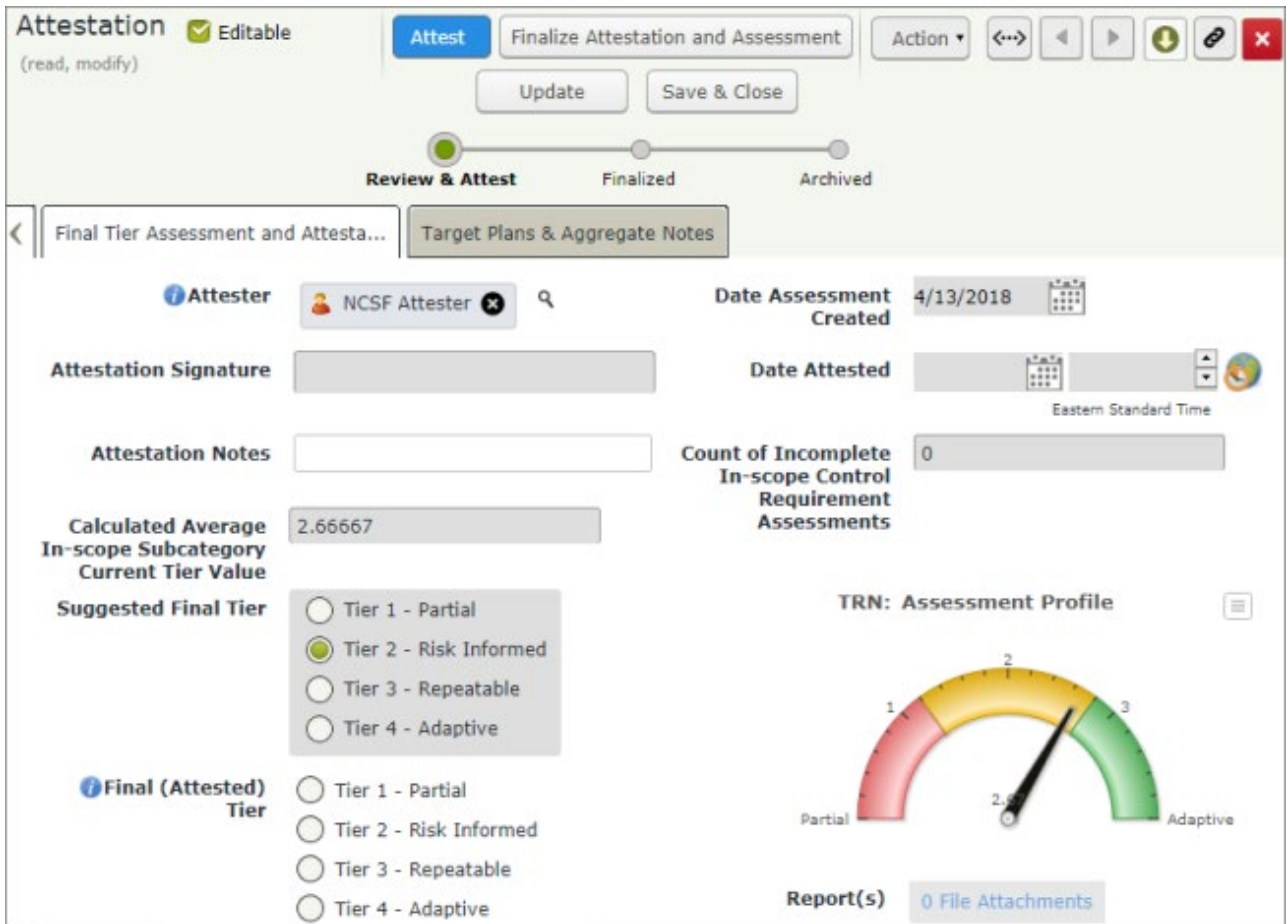
1. Sign in to Rsam as the *NCSF Assessor*. Provide the **Username** as *r_ncsf_assessor* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator Home page opens listing all the NCSF Profile Assessments defined.
3. On the **Assessment Navigator** page, select the required NCSF Profile Assessment and click **Actions > Request Attestation**. A confirmation message appears stating that an Assessment/Attestation record will be created to finalize the assessment.
Alternatively, you can open the assessment and click  and select **Request Attestation** from within the Object Details page.
4. Click **OK** in the confirmation message pop up that appears.
The Profile moves to the **Pending Attestation** state and an Attestation record is generated.

Step 2: Attesting to an NCSF Profile Assessment

To attest to an NCSF Profile Assessment, perform the following steps:

1. Sign in to Rsam as the *NCSF Attester*. Provide the **Username** as *r_ncsf_attester* and **Password** as *password*.

2. Navigate to **NIST Cybersecurity Framework > Assessment/Profile Navigator**. The Assessment Navigator Home page opens listing all the Assessment Profiles defined.
3. On the **Assessment Navigator** page, double-click the required Assessment Object in the **Pending Attestation** state. The Object Details page opens listing details of the NCSF Profile Assessment.
4. Click **Attestations (x)** link in the **Requirements** section. The **Attestations** page opens.
5. Double-click the attestation record to open it. The record opens showing the **Final Tier Assessment and Attestation** tab.
6. Select the final tier for the Assessment from the values corresponding to the **Final (Attested) Tier** tab. This value determines the overall tier for the Assessment.
7. Provide values for other fields as required.



Attestation Editable (read, modify)

Attest Finalize Attestation and Assessment Action <=> < > <=> <=> <=>

Update Save & Close

Review & Attest Finalized Archived

Final Tier Assessment and Attesta... Target Plans & Aggregate Notes

Attester NCSF Attester

Date Assessment Created 4/13/2018

Attestation Signature

Date Attested

Attestation Notes

Count of Incomplete In-scope Control Requirement Assessments 0

Calculated Average In-scope Subcategory Current Tier Value 2.66667

Suggested Final Tier

- Tier 1 - Partial
- Tier 2 - Risk Informed
- Tier 3 - Repeatable
- Tier 4 - Adaptive

Final (Attested) Tier

- Tier 1 - Partial
- Tier 2 - Risk Informed
- Tier 3 - Repeatable
- Tier 4 - Adaptive

TRN: Assessment Profile

Partial 1 2 3 Adaptive

Report(s) 0 File Attachments

8. Click **Target Plans & Aggregate Notes** tab to view notes and status change messages related to the control requirement records and Assessment Profile.
9. Click **Finalize Attestation and Assessment**. Click **OK** in the confirmation message pop up that appears. The record moves to the **Finalized** state.
Automatically, the Assessment Profile also moves to the **Finalized** state and the Final Tier value is appended to the Assessment Profile.
Alternatively, you can also click **Attest** and the record moves to the **Finalized** state, but the Profile remains in the **Pending Attestation** state. Now an NCSF Owner must log in and click **Finalize** in the Assessment Profile to move the profile to the **Finalized** state.

Note: An NCSF Attester can add more Attestation records, if required, by clicking **Add > Attestation**. When a new record is attested and finalized, if any prior records are available in the **Finalized** state, those records move to the **Archived** state.

Finalizing NCSF Assessments

An active NCSF Profile Assessment has a number of control requirements associated with it. When all the associated control requirements are reviewed and approved and are in the Finalized state, the NCSF Profile Assessment moves to the **Finalized** state automatically.

The following figure shows details of an NCSF Profile Assessment in the Finalized state.

Assessment Framework (NCSF): TRN: Assessment Profile

Workflow State: Finalized Target Tier: Tier 3 - Repeatable Owner: NCSF Owner Assessment End Date:	Name: TRN: Assessment Profile Final Tier: Tier 2 - Risk Informed Assessment Start Date:
--	---

Cybersecurity Profile

Name	Questionnaire	State			
TRN: Assessment Profile	1 of 1 answered	Finalized			

Cybersecurity Core

[Control Requirements \(3\)](#)

[Attestations \(1\)](#)

In-Scope Control Requirement Assessment Progress

Finalized, 3

In-Scope Control Requirements by NCSF Function

1-Identity (ID)

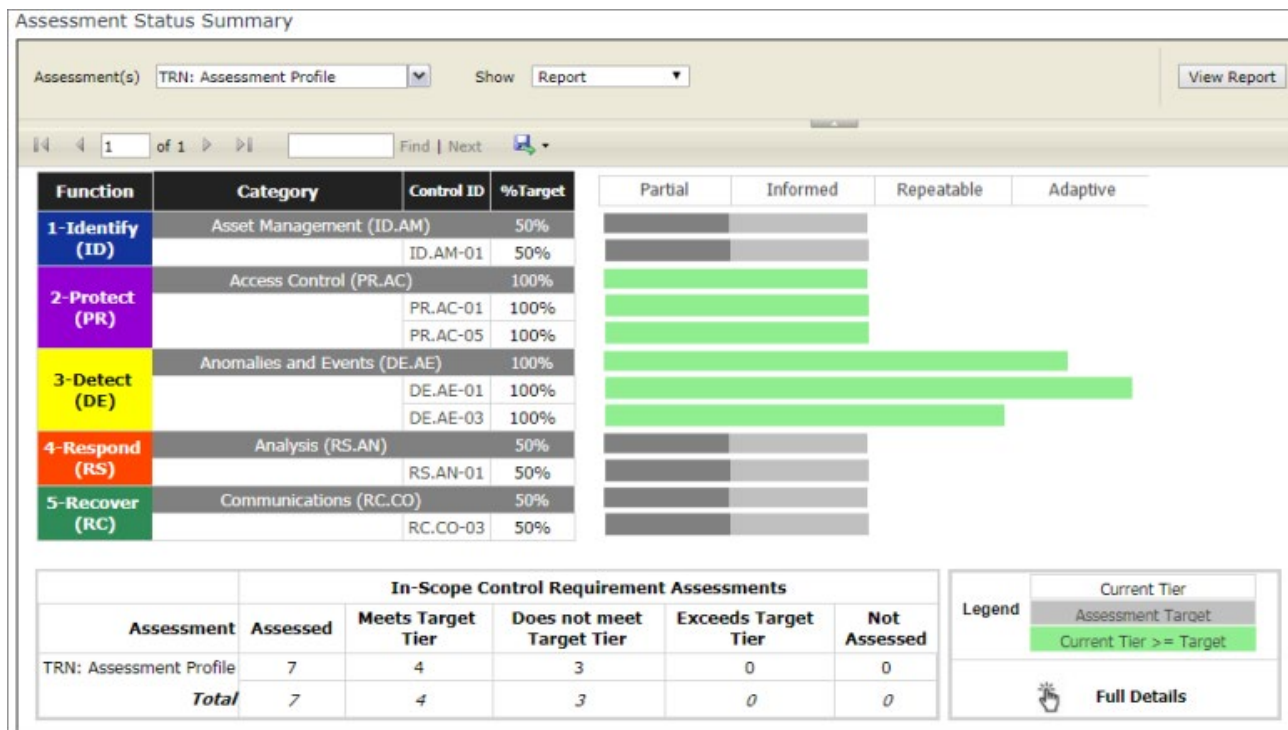
■ Tier 3 - Repeatable
 ■ Tier 2 - Risk Informed

NCSF Assessment Status Summary

Rsam provides an Assessment Status Summary Report, which provides an overview of the NCSF Assessments in the system. This report provides a birds-eye-view of the gaps and tier assessments for the NCSF assessments and related control requirements. It is highly useful to executive management when analysing the NCSF Profile Assessments in the system, where users with access can select all the required assessments simultaneously and view the comparative results.

The report can also be downloaded and shared with stakeholders for any analysis or informational purposes. To access the report, click **NIST Cybersecurity Framework > Target Tier Progress Drill-Down**.

The following image shows an example NCSF Assessment Status Summary.



Working with Assessment Status Summary

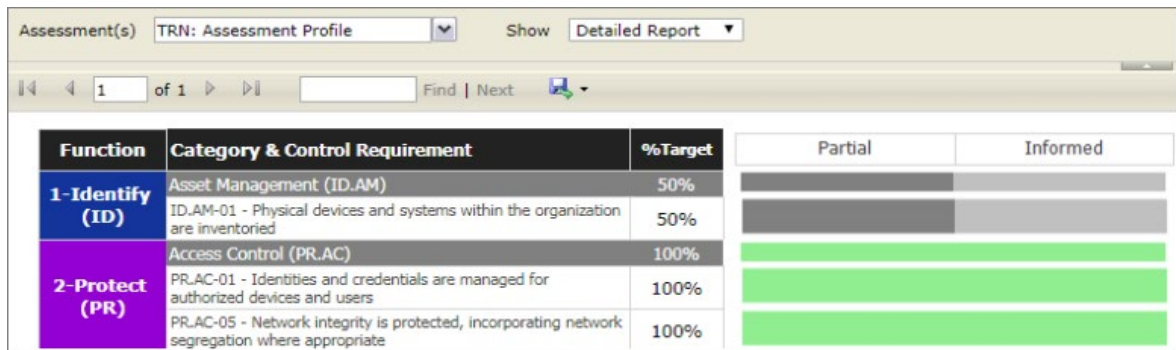
The following section explains the components of the report and how to use it:

- [Generating a Report](#)
- [NCSF Function and Category Details](#)
- [Overall Summary of Assessments](#)

Generating a Report

To generate a report, perform the following steps:

1. Sign in to Rsam as a user with access to the Assessment Status Summary.
2. Navigate to **NIST Cybersecurity Framework > Target Tier Progress Drill-Down**.
3. In the Report pane, select the required NCSF Profile Assessment(s), of which you want to view the summary, in the **Assessment(s)** field.
4. Select the required view from the **Show** field. The values available are as follows:
 - **Report** - Displays the % Target and tier corresponding to each Control Requirement for the selected NCSF Profile Assessment(s).
 - **Summary Report** - Provides a summary of the selected assessments with no granular data. Displays the overall tier and % Target for the Function as a whole.
 - **Detailed Report** - Displays detailed data for the selected assessment(s). Users can view the descriptions of all articles and corresponding tier assignments.



Function	Category & Control Requirement	%Target	Partial	Informed
1-Identify (ID)	Asset Management (ID.AM)	50%	<div style="width: 50%; background-color: #ccc;"></div>	<div style="width: 50%; background-color: #ccc;"></div>
	ID.AM-01 - Physical devices and systems within the organization are inventoried	50%	<div style="width: 50%; background-color: #ccc;"></div>	<div style="width: 50%; background-color: #ccc;"></div>
2-Protect (PR)	Access Control (PR.AC)	100%	<div style="width: 100%; background-color: #90EE90;"></div>	<div style="width: 100%; background-color: #90EE90;"></div>
	PR.AC-01 - Identities and credentials are managed for authorized devices and users	100%	<div style="width: 100%; background-color: #90EE90;"></div>	<div style="width: 100%; background-color: #90EE90;"></div>
	PR.AC-05 - Network integrity is protected, incorporating network segregation where appropriate	100%	<div style="width: 100%; background-color: #90EE90;"></div>	<div style="width: 100%; background-color: #90EE90;"></div>

5. Click **View Report**. The pane refreshes to show the report based on the selections.

NCSF Function and Category Details

This section categorizes the tier assignments for each article based on the Function and Category to which it belongs and represents values in **percentages** and **graphically**. In a Report or Detailed view, the tier assignments shown are as follows:

- **For each applicable Control Requirement / Article.**
- **At the Function level** - after calculating the tier based on all Control Requirements / Articles in that category.
- **At the Category level** - after calculating the tier based on all Control Requirements / Articles for each **Function** in that chapter.

Click the graphical bars or values to view additional details. The details provided in this report depend on the selected Function, Category, or Subcategory.

Assessment Summary Details								
Function		3-Detect (DE)						
Category		Anomalies and Events (DE.AE)						
Control Requirements		DE.AE-01 - A baseline of network operations and expected data flows for users and systems is established and managed						
<small>* Assessments > 100% of Target are evaluated as 100% of Target ** Un-assessed Control Requirements (Current Tier = 0%) are not included in the average *** Progress is the % greater than the Current Tier Assessment -or- additional progress toward reaching the Target Tier</small>								
Assessment Name	Category	Control ID	Current Tier	Progress***	Current Tier Weight	Target Tier	Target Tier Weight	% of Target
TRN: Assessment Profile	Anomalies and Events (DE.AE)	DE.AE-01	Tier 4 - Adaptive	0%	400	Tier 4 - Adaptive	400	100%
Average:					400		400	100%*
Summary (Average)					400		400	100%
There are no Action Plans to list for this selection								

Overall Summary of Assessments

The last section in the report shows a summary of all control requirements for the selected assessments, with **numerical values**.

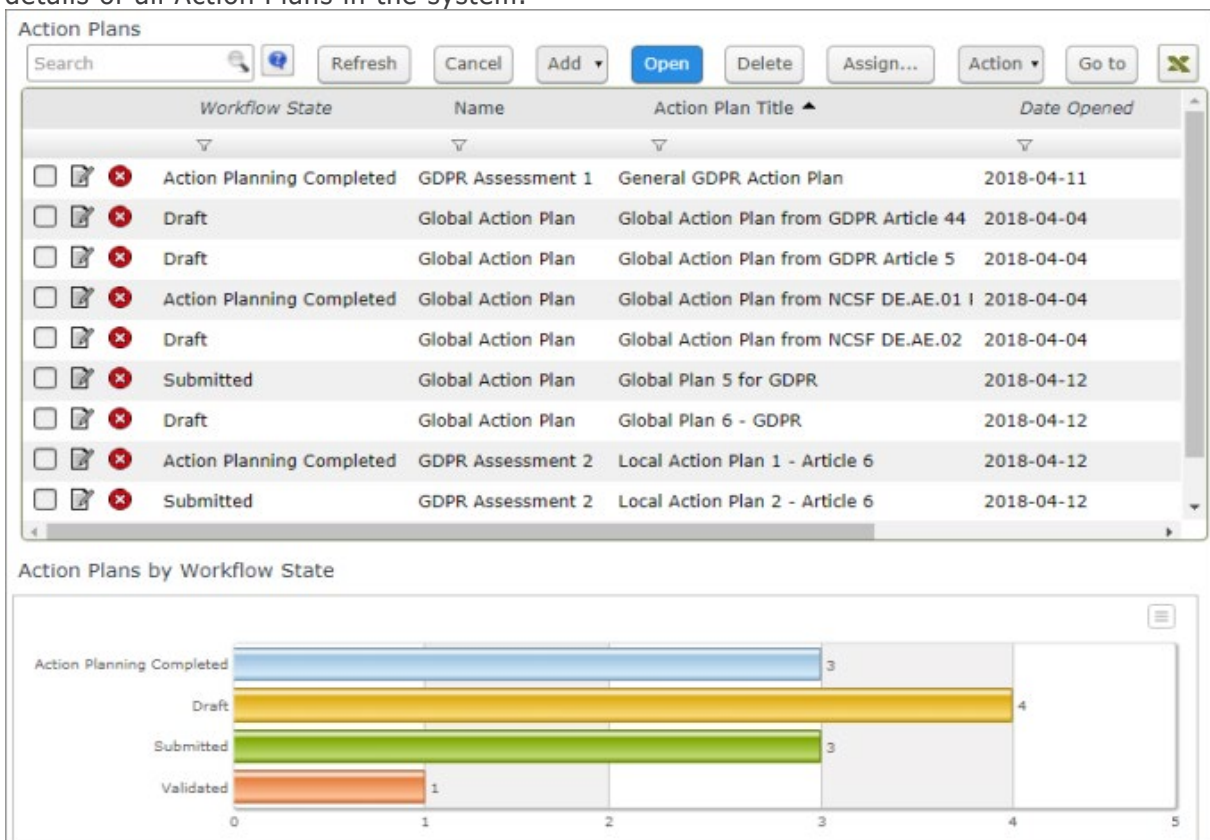
Assessment	In-Scope Control Requirement Assessments				
	Assessed	Meets Target Tier	Does not meet Target Tier	Exceeds Target Tier	Not Assessed
Assessment 1	4	2	2	1	0
Assessment 2	6	3	3	0	0
Assessment 3	19	10	9	0	0
Total	29	15	14	1	0

4. Provide values for the required fields.
5. Click the **Related Control Requirements** tab.
6. Click **Add** corresponding to the **Control Requirements for NCSF Action Plans** section and map control requirements to the plan, as required.
7. Click **Submit**. A confirmation message appears stating that the plan will be moved to the **Submitted** state.
8. Click **OK** in the dialog box. The plan is saved in the **Submitted** state.

Approving an Action Plan

To approve an action plan, perform the following steps:

1. Sign in to Rsam as the *NCSF Reviewer*. Provide the **Username** as *r_ncsf_reviewer* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Action Planning**. A page appears listing details of all Action Plans in the system.



The screenshot displays the 'Action Plans' management interface. At the top, there is a search bar and several action buttons: Refresh, Cancel, Add, Open, Delete, Assign..., Action, and Go to. Below this is a table with the following columns: Workflow State, Name, Action Plan Title, and Date Opened. The table contains 10 rows of data, each with a checkbox, a document icon, and a red 'x' icon. Below the table is a bar chart titled 'Action Plans by Workflow State' showing the count of plans for each state: Action Planning Completed (3), Draft (4), Submitted (3), and Validated (1).

Workflow State	Name	Action Plan Title	Date Opened
Action Planning Completed	GDPR Assessment 1	General GDPR Action Plan	2018-04-11
Draft	Global Action Plan	Global Action Plan from GDPR Article 44	2018-04-04
Draft	Global Action Plan	Global Action Plan from GDPR Article 5	2018-04-04
Action Planning Completed	Global Action Plan	Global Action Plan from NCSF DE.AE.01	2018-04-04
Draft	Global Action Plan	Global Action Plan from NCSF DE.AE.02	2018-04-04
Submitted	Global Action Plan	Global Plan 5 for GDPR	2018-04-12
Draft	Global Action Plan	Global Plan 6 - GDPR	2018-04-12
Action Planning Completed	GDPR Assessment 2	Local Action Plan 1 - Article 6	2018-04-12
Submitted	GDPR Assessment 2	Local Action Plan 2 - Article 6	2018-04-12

Workflow State	Count
Action Planning Completed	3
Draft	4
Submitted	3
Validated	1

3. Select the required action plan, review the details, and click **Accept**.
4. Click **OK** in the confirmation dialog that appears. The action plan moves to the **Completed** state.

Validating an Action Plan

After an Action Plan has been approved, an Assessor must validate the plan. To validate an Action Plan, perform the following steps:

1. Sign in to Rsam as the *NCSF Assessor*. Provide the **Username** as *r_ncsf_assessor* and **Password** as *password*.
2. Navigate to **NIST Cybersecurity Framework > Action Planning**. A page appears listing details of all Action Plans in the system.
3. Select the required Action Plan in the **Completed** state and select **Action > Action Plan Validated**. The plan is validated and moves to the **Validated** state.

Appendix 2: Rsam Documentation

NIST Cybersecurity Framework Baseline Configuration Guide

To learn more about the pre-configurations in the NIST Cybersecurity Framework, refer the *NIST Cybersecurity Framework Baseline Configuration Guide*. You should have received the *NIST Cybersecurity Framework Baseline Configuration Guide* along with the NIST Cybersecurity Framework sandbox. If not, please contact your Rsam Customer Representative to obtain an electronic copy of the *NIST Cybersecurity Framework Baseline Configuration Guide*.

Online Help

This tutorial provides the step-by-step instructions for the Rsam NIST Cybersecurity Framework module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **Username** as *r_admin* and **Password** as *password*.
2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.

