



HITRUST MyCSF Module

Step-by-Step Tutorial

Document Version: 2017.12.10 | December 2017

Rsam © 2017. All rights reserved

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

Contents

- About Rsam Tutorials 3
- Access the Rsam Sandbox Environment 4
 - Rsam Environment..... 4
 - Login Page 4
- HITRUST MyCSF Module..... 5
 - Overview 5
 - Hitrust MyCSF Workflow 5
 - User Accounts 8
 - High-Level Steps 8
- Step-by-Step Procedure..... 9
 - Step 1: Create a HITRUST CSF Assessment 9
 - Step 2: Answer a HITRUST CSF Assessment 13
 - Step 3: Review Hitrust CSF Assessment Answers 15
 - Step 4: Create and Complete CAPs..... 17
- Appendix 1: Email Notifications and Offline Decision Making 21
 - Setting up Email Addresses 21
 - Offline Decision Making 22
- Appendix 2: Rsam Documentation 23
 - HITRUST MyCSF Module Baseline Configuration Guide 23
 - Inline Help 23

About Rsam Tutorials

The Rsam module step-by-step tutorials are designed to provide you the opportunity to learn about a specific Rsam module, and to gain basic familiarity with the user experience. The Rsam platform is highly configurable and is capable of handling both simple and comprehensive applications. Rsam 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 a common, out-of-the-box functionality within a given Rsam module, allowing you to get immediate hands-on familiarity with the concepts and interface.

Access the Rsam Sandbox Environment

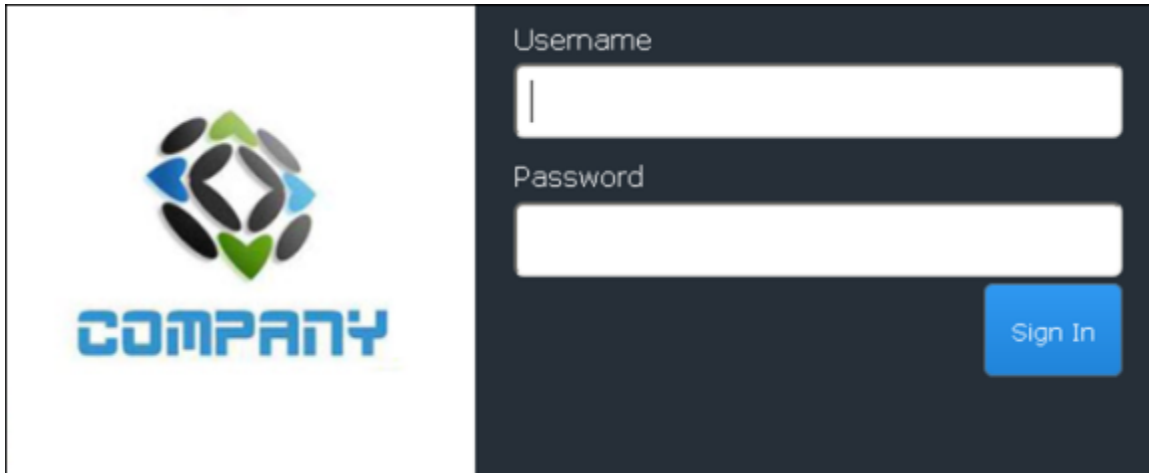
Rsam Environment

Rsam module step-by-step tutorials are designed to work with the out-of-the-box Rsam configuration. You may be following 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 via email along with this tutorial guide. Otherwise, you may contact your Rsam administrator for the URL to access your Rsam instance.

If you are leveraging 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 Representative with any questions.

Login Page

Tutorials leverage pre-defined accounts that require authentication. Because your Rsam HITRUST MyCSF Module sandbox environment is for demonstration purposes, manual authentication is required via the default sign-in screen that opens when you access the secure URL.



Like most elements in Rsam, the login 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. In addition, you can embed your own branding and logo on the login page.

HITRUST MyCSF Module

Overview

HITRUST CSF is a popular security framework with wide-spread adoption across US-based healthcare organizations. It provides them with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. Developed jointly by healthcare and information security professionals, the HITRUST CSF rationalizes relevant regulations and standards into a single overarching security framework.

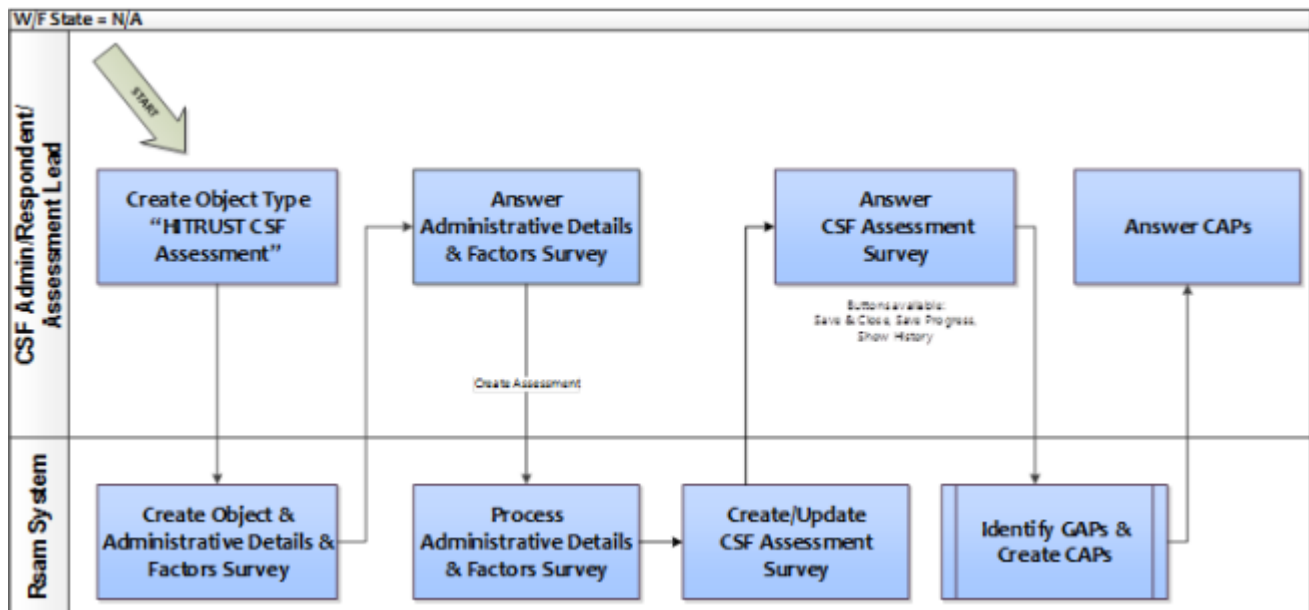
Rsam has partnered with HITRUST to create the HITRUST MyCSF module, which offer clients a nearly identical user experience to the HITRUST CSF instance. Rsam's HITRUST MyCSF is a self-contained module that stands on its own to allow clients the opportunity to perform the same assessment they would on the HITRUST CSF site with the added HITRUST feature of MyCSF Plus, the capability to include CAP (Corrective Action Plan) management.

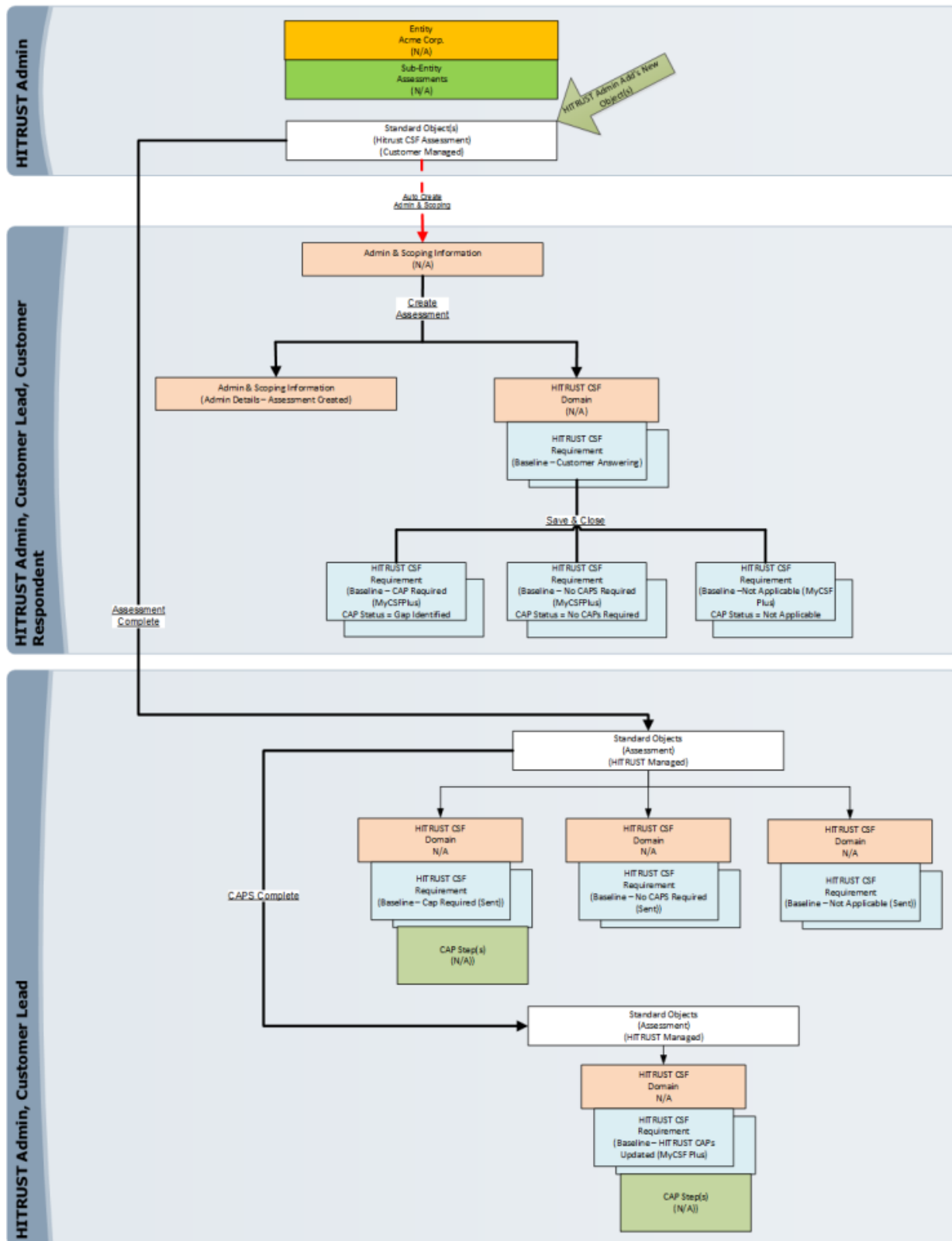
The Rsam HITRUST MyCSF module provides the following capabilities and benefits:

1. Dashboards to track and understand compliance, gaps, controls, and scores.
2. Locally generated reports that are duplicates of the reports found on the HITRUST CSF site.
3. All requirements and mappings to Level(s) 1, 2, and 3.
4. CAP Management.

Hitrust MyCSF Workflow

The following diagram depicts the out-of-the-box workflow:





User Accounts

User accounts are required for the individuals that are authorized to access a specific Rsam template. The Rsam sandbox for HITRUST MyCSF comes with pre-populated sample accounts that include the following:

Account ID	User	Business Responsibilities
r_csf_admin	CSF Admin	This user is responsible for overall administration of CSF assessments. Hence, has the ability to create and answer CSF assessments, and complete CAPs.
r_csf_respondent	CSF Respondent	This user is responsible for answering CSF assessment requirements.
r_csf_lead	CSF Lead	This user can perform the same activities like the CSF Admin user. This tutorial does not use this user to execute any of the steps. Depending on your workflow and need, you may use this user in your organization.

High-Level Steps

The following is a high-level list of the steps we will follow in the step-by-step portion of this tutorial.

Step	User	Description
Step 1: Create a HITRUST CSF Assessment	CSF Admin	In this step, the CSF Admin user creates a HITRUST CSF assessment.
Step 2: Answer a HITRUST CSF Assessment	CSF Respondent	In this step, the CSF Respondent user responds to the maturity levels for each requirement in the assessment.
Step 3: Review HITRUST CSF Assessment Answers	CSF Admin	In this step, the CSF Admin user reviews the answers submitted by the CSF Respondent user.
Step 4: Create and Complete Corrective Action Plan(s) (CAPs)	CSF Admin	In this step, the CSF Admin user creates CAPs for all requirements that were identified as a Gap.

Step-by-Step Procedure

This section contains the workflow steps we will follow in this tutorial. The path covered in this tutorial will walk you through the steps to create a HISTRUST CSF assessment, answer CSF requirements, and complete CAPs. This path was chosen as it is a common path to follow, though you are welcome to explore other paths as well.

From this point forward, we will provide the steps that are required to complete this tutorial. Before you begin to practice each step, consider the following underlying capabilities:

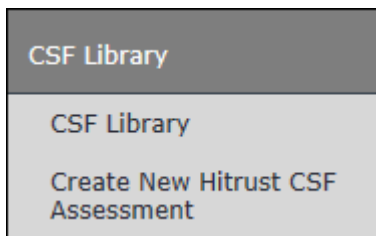
- a. Practicing each step requires a different user account as mentioned in the High-Level Steps section. However, you may execute all the steps with the CSF Administrator user credentials in one session if desired.
- b. Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your workflow users receive the notifications while practicing the steps, please see [Setting up Email Addresses](#).

Step 1: Create a HISTRUST CSF Assessment

In this step, you will log in to Rsam as the CSF Administrator user to create a HISTRUST CSF assessment.

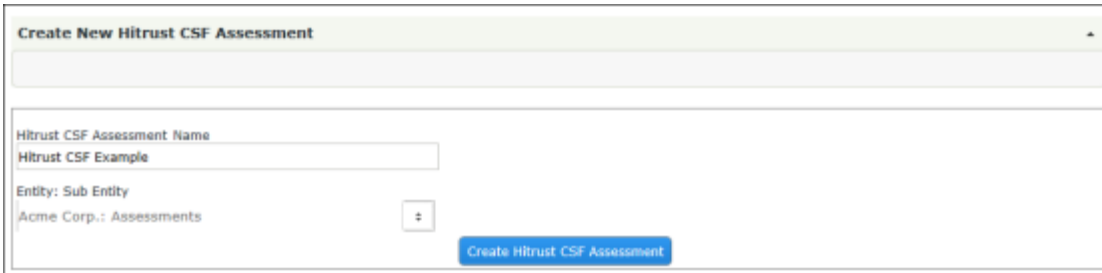
Procedure:

1. Sign in as the CSF Admin user. Enter **Username** as **r_csf_admin** and **Password** as **password**.
2. From within the navigation panel on the left-hand side of the screen, navigate to **CSF Library** > **Create New Hitrust CSF Assessment**.

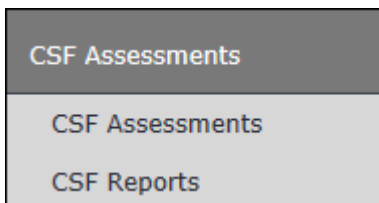



The Create New Hitrust CSF Assessment home page appears.

3. Enter **Hitrust CSF Example** in the **Hitrust CSF Assessment Name** attribute.




4. Click **Create Hitrust CSF Assessment**.
5. Navigate to **CSF Assessments > CSF Assessments**.



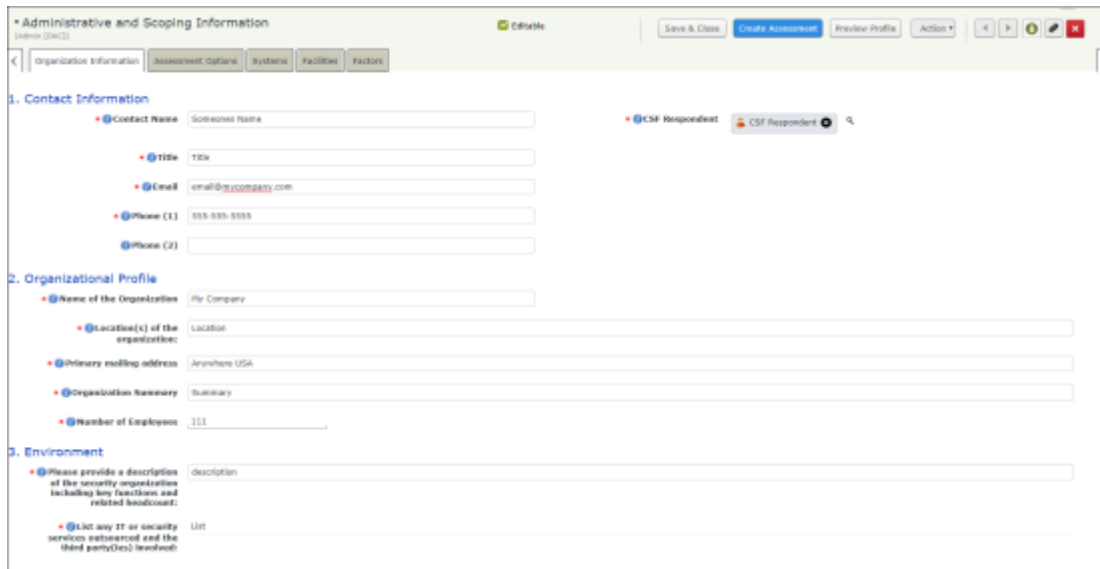
6. Open the "Hitrust CSF Example" object by using one of the following methods:
 - Double-click the "Hitrust CSF Example" object .
 - Select the "Hitrust CSF Example" object and click **Open**.
 - Click the  icon in the "Hitrust CSF Example" object row.
The "Hitrust CSF Example" object details appear.

7. Click **Administrative Details & Factors**.



The **Administrative and Scoping Information** record opens with the **Organization Information** tab selected.

8. On the **Organization Information** tab, enter all the required information marked with asterisk (*).



Administrative and Scoping Information
(read, modify, delete) Editable

Save & Close Create Assessment Preview Profile Action

Organization Information Assessment Options Systems Facilities Factors

1. Contact Information

- @Contact Name: Someone's Name
- @Title: Title
- @Email: email@mycompany.com
- @Phone (1): 555-555-5555
- @Phone (2):

2. Organizational Profile

- @Name of the Organization: My Company
- @Location(s) of the organization: Location
- @Primary mailing address: Anywhere USA
- @Organization Summary: Summary
- @Number of Employees: 111

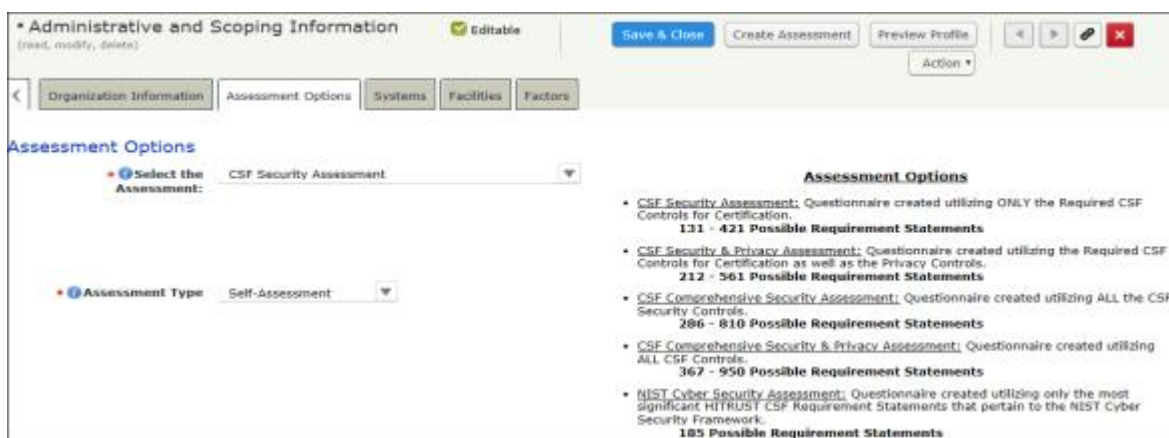
3. Environment

- @Please provide a description of the security organization including any functions and related hardware: description
- @List any IT or security services outsourced and the third party(ies) involved: Unit

9. Click the **Assessment Options** tab and enter the values for the fields listed in the following table.

Field	Value
Select the Assessment	*CSF Security Assessment
Assessment Type	*Self-Assessments (Auto-populates) (Select only Self-Assessments; 3rd party is only for use when using HITRUST system not an on premises system)

**Values selected for the sake of completing this tutorial. If desired, you may select a different value .*



Administrative and Scoping Information
(read, modify, delete) Editable

Save & Close Create Assessment Preview Profile Action

Organization Information Assessment Options Systems Facilities Factors

Assessment Options

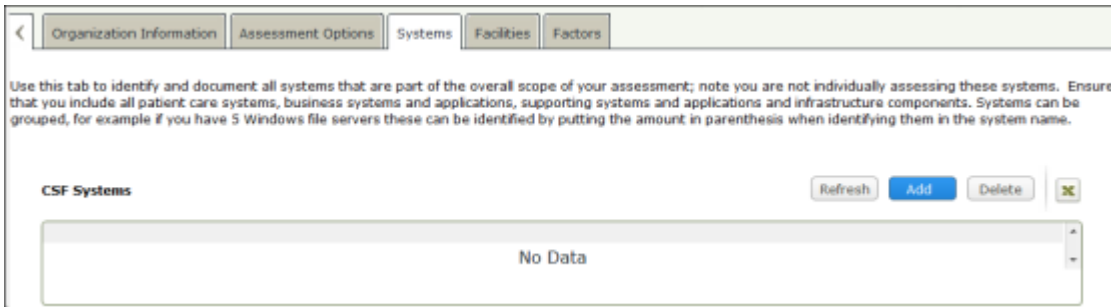
- Select the Assessment: CSF Security Assessment
- Assessment Type: Self-Assessment

Assessment Options

- **CSF Security Assessment:** Questionnaire created utilizing ONLY the Required CSF Controls for Certification.
131 - 421 Possible Requirement Statements
- **CSF Security & Privacy Assessment:** Questionnaire created utilizing the Required CSF Controls for Certification as well as the Privacy Controls.
212 - 561 Possible Requirement Statements
- **CSF Comprehensive Security Assessment:** Questionnaire created utilizing ALL the CSF Security Controls.
286 - 810 Possible Requirement Statements
- **CSF Comprehensive Security & Privacy Assessment:** Questionnaire created utilizing ALL CSF Controls.
367 - 950 Possible Requirement Statements
- **NIST Cyber Security Assessment:** Questionnaire created utilizing only the most significant HITRUST CSF Requirement Statements that pertain to the NIST Cyber Security Framework.
185 Possible Requirement Statements

10. Click the **Systems** tab. Here, you may add all systems that you want to include as part of the overall scope of your assessment. To add a system, click **Add** and select **CSF Systems**. In the

CSF Systems (new) record, enter all the fields that are necessary to you and click **Save & Close**.



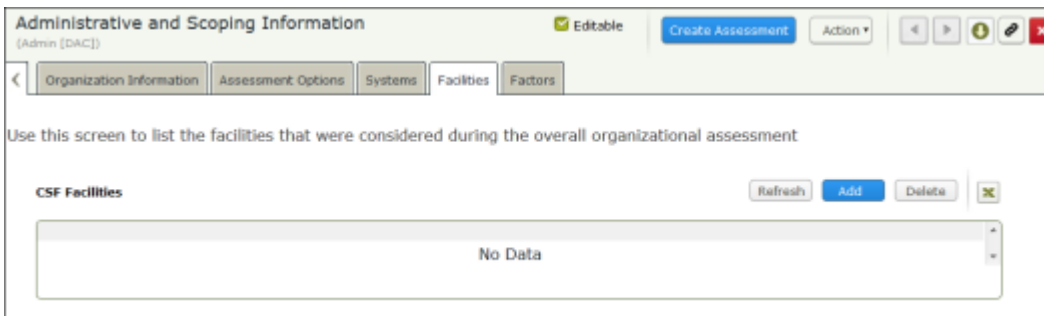
Use this tab to identify and document all systems that are part of the overall scope of your assessment; note you are not individually assessing these systems. Ensure that you include all patient care systems, business systems and applications, supporting systems and applications and infrastructure components. Systems can be grouped, for example if you have 5 Windows file servers these can be identified by putting the amount in parenthesis when identifying them in the system name.

CSF Systems

Refresh Add Delete

No Data

11. Click the **Facilities** tab. Here, you may add all the facilities that you want to include as part of your organization assessment. To add a CSF facility, click **Add** and select **CSF Facilities**. In the **CSF Facilities (new)** record, enter all the fields that are necessary to you and click **Save & Close**.



Administrative and Scoping Information Editable Create Assessment Action

Use this screen to list the facilities that were considered during the overall organizational assessment

CSF Facilities

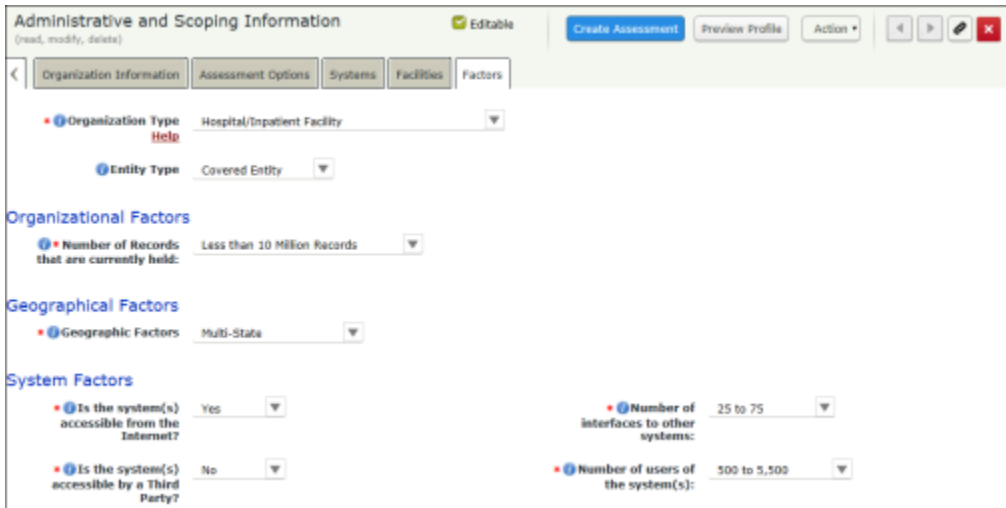
Refresh Add Delete

No Data

12. Click the **Factors** tab and perform the following steps:
 - a. Enter the values for the fields listed in the table below:

Field	Value
Organization Type	*Hospital/Inpatient Facility
Entity Type	*Covered Entity

**Values selected for the sake of completing this tutorial. If desired, you may select a different value.*
 - b. Complete all other required factors marked with asterisk (*).




When you select **Unknown** under **Organizational Factors**, you will be provided with another attribute (choice); these choices will (in combination with the type of assessment you are performing) determine the number and level of requirements you receive.

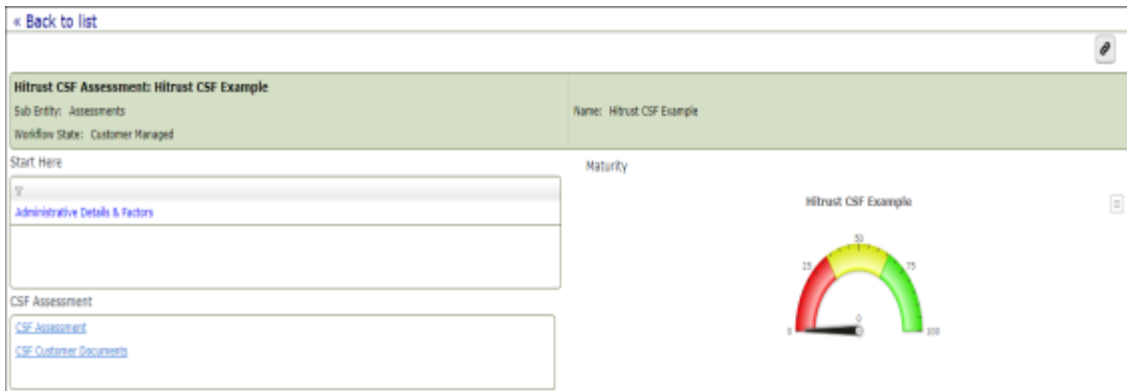
13. Click **Create Assessment**.

Step 2: Answer a HITRUST CSF Assessment

In this step, you will log in to Rsam as the CSF Respondent user to answer the HITRUST CSF assessment.

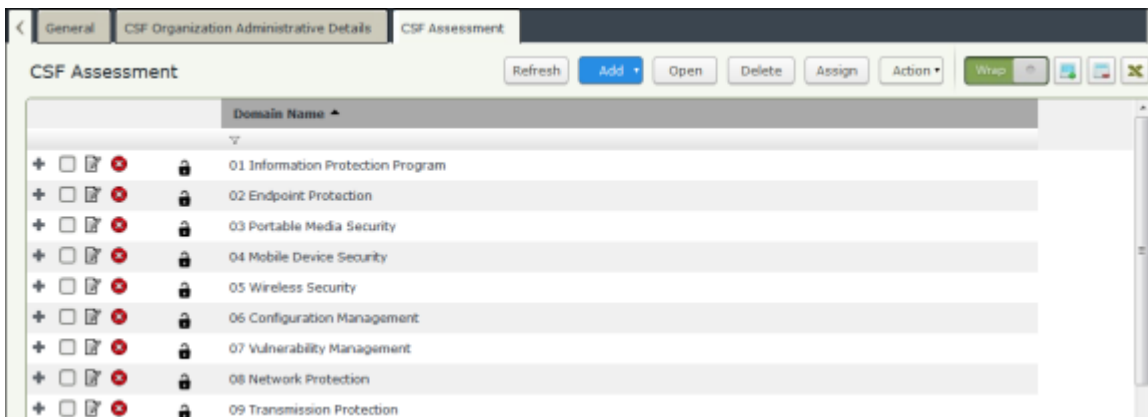
Procedure:

1. Sign in as the CSF Respondent user. Enter **Username** as **r_csf_respondent** and **Password** as **password**.
2. From within the navigation panel on the left-hand side of the screen, navigate to **CSF Assessments > CSF Assessments**.
3. Open the "Hitrust CSF Example" object by using one of the following methods:
 - Double-click the "Hitrust CSF Example" object.
 - Select the "Hitrust CSF Example" object and click **Open**.
 - Click the  icon in the "Hitrust CSF Example" object row.
4. Under **CSF Assessment**, click the **CSF Assessment** link.



The CSF Assessment record category opens with a list of domains.

- Click **+** to expand the first domain.



Domain Name	
+	01 Information Protection Program
+	02 Endpoint Protection
+	03 Portable Media Security
+	04 Mobile Device Security
+	05 Wireless Security
+	06 Configuration Management
+	07 Vulnerability Management
+	08 Network Protection
+	09 Transmission Protection

- Double-click the first record under the domain to open the requirement record.

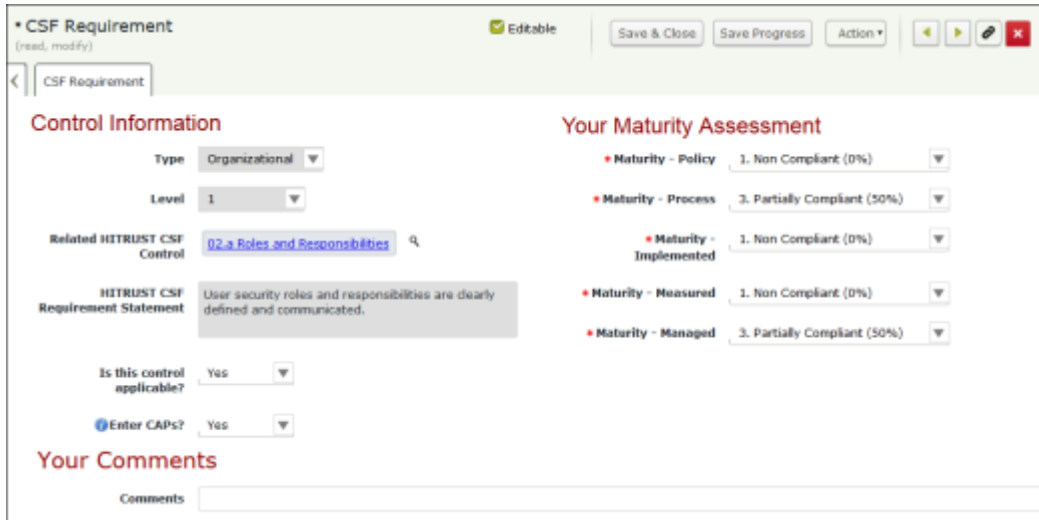
Domain Name

01 Information Protection Program

Response Status	CAP Status	In Scope	Level	CSF Requirement Statement
<div><div></div><div></div><div></div><div></div></div>		In scope	1	The organization has a formal information framework that is reviewed and updated a
<div><div></div><div></div><div></div><div></div></div>		In scope	1	User security roles and responsibilities are
<div><div></div><div></div><div></div><div></div></div>		In scope	1	The organization has an information secu

The **CSF Requirement** record opens with the **CSF Requirement** tab selected.

- On the **CSF Requirement** tab and enter all the responses marked with asterisk (*).



**If you change "Is this control applicable?" to No, you will be required to provide a comment on why this requirement is not applicable*

8. Click **Save & Close** to save the baseline response.
9. Repeat steps 6 through 8 to answer the rest of the CSF requirements under the domain.
10. Open each domain and answer all CSF requirements. When a requirement has been answered, the **Response Status** is set to "Complete." Please check to make sure that the CSF requirements have the Response Status "Complete."

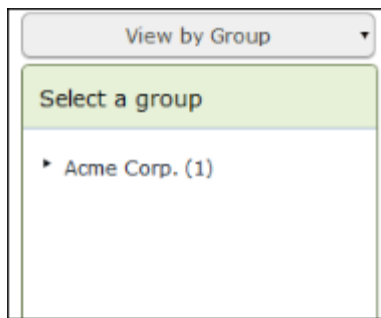
The CAP Status will indicate whether the requirement has been identified as a Gap or No CAPs Required.

Step 3: Review Hitrust CSF Assessment Answers

After your respondent has answered the CSF assessment, you will review the CSF assessment answers.

Procedure:


1. Sign in as the CSF Admin user. Enter **Username** as **r_csf_admin** and **Password** as **password**.
2. From within the navigation panel on the left-hand side of the screen, navigate to **CSF Dashboards > CSF Gaps and Risks**.
3. From within the navigator, expand **Acme Corp**.



4. Select **Assessments**.

The assessments of object type "Hitrust CSF Assessment" appear.

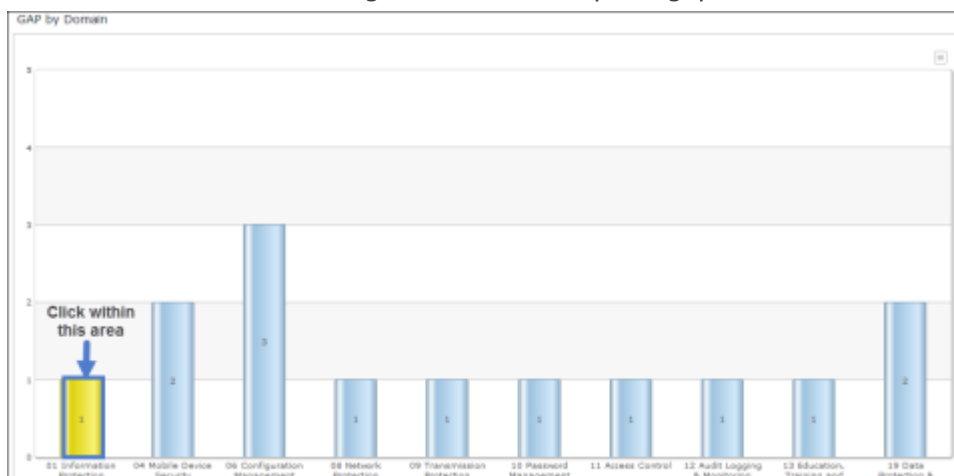
5. Open the "Hitrust CSF Example" object by using one of the following methods:

- Double-click the "Hitrust CSF Example" object .
- Select the "Hitrust CSF Example" object and click **Open**.
- Click the  icon in the "Demo for Hitrust CSF Assessment" object row.



Dashboards illustrating compliance, gaps, and risks per domain appear.

4. Under **Gap by Domain**, click on the bar. As part of this tutorial, we will click on the "Information Protection Program" bar to complete gaps in this domain.



** You may have different domains depending on the type of assessment you chose and the factors you indicated when you created the assessment.*

The "MyCSF: GAP by Domain" chart displays CSF requirements in the domain that have gaps.

6. Double-click the CSF assessment record.

Search Name: MyCSF: GAP by Domain (chart)

Search Refresh Cancel Add Open Delete Assign... Action Go to Search Criteria Save Save Search As

Select a group	Domain Name	GAP Rating
01 Information Protection Program (1)		
04 Mobile Device Security (2)		
06 Configuration Management (2)		
08 Network Protection (1)		

Record Category	Record Type	Name	Workflow State	Response Status
CSF Assessment	CSF Requirement	Hitrust CSF Example	Baseline - Cap Required	Complete

The **CSF Requirement** record opens with the **CSF Requirement** tab selected.

7. Review the maturity answers for policy, process, implemented, measures, and managed.
8. Once you've reviewed, the requirement records the assessment is ready for completion.
9. Navigate to CSF Assessments Tab under CSF Assessments and select the row for the assessment you wish to complete and click Action then click Assessment Complete.

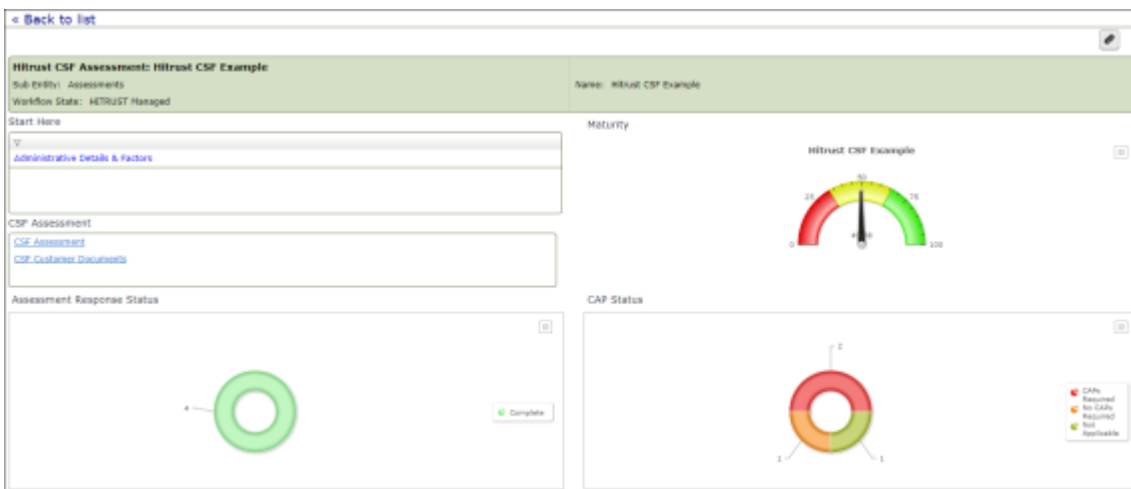
MyCSF: Assessments (nav) Search Refresh Cancel Add Open Delete Assign... Action Assessment Complete

Sub Entity	Name	Workflow State	Object Type
Assessments	B_1801001	Customer Managed	Hitrust CSF Assessment
Assessments	C_1801001	Customer Managed	Hitrust CSF Assessment
Assessments	Hitrust CSF Example	Customer Managed	Hitrust CSF Assessment

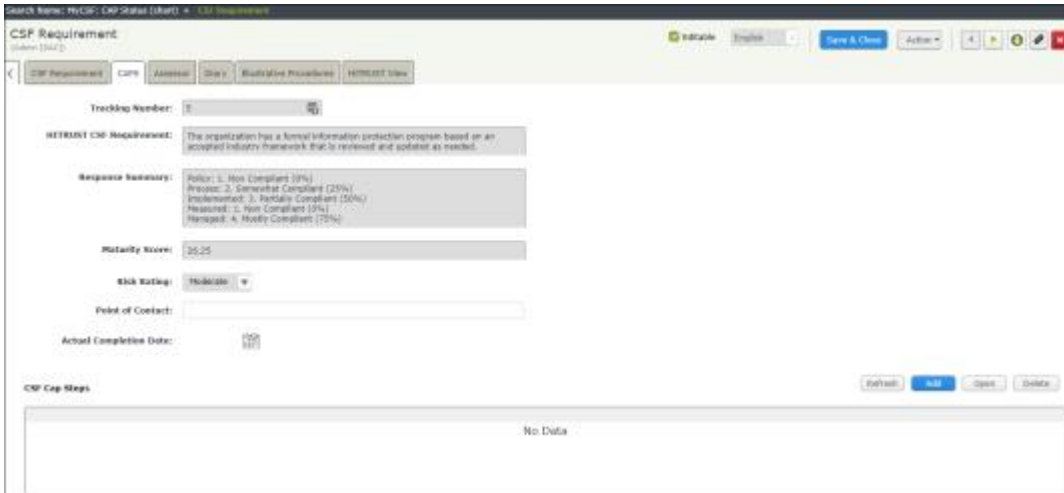
Step 4: Create and Complete CAPs

In this step, we will create and complete CAPs for all requirements that were identified as Gaps. By staying signed in as the CSF Admin user, you will complete the following steps.

1. Open the assessment and click the CAPs Required section of the donut chart.



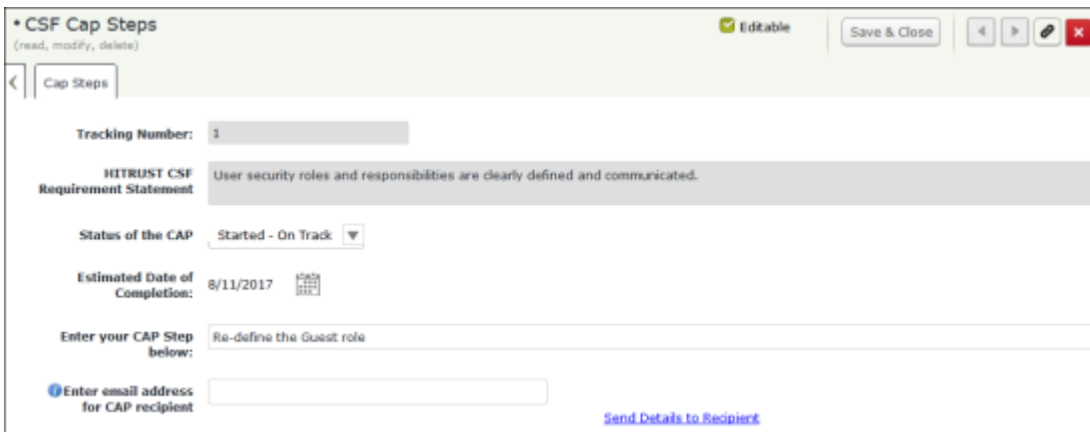
2. Open each record where a CAP is required.
3. Click the CAPS tab.
4. Click the Add button to add a CAP Step.



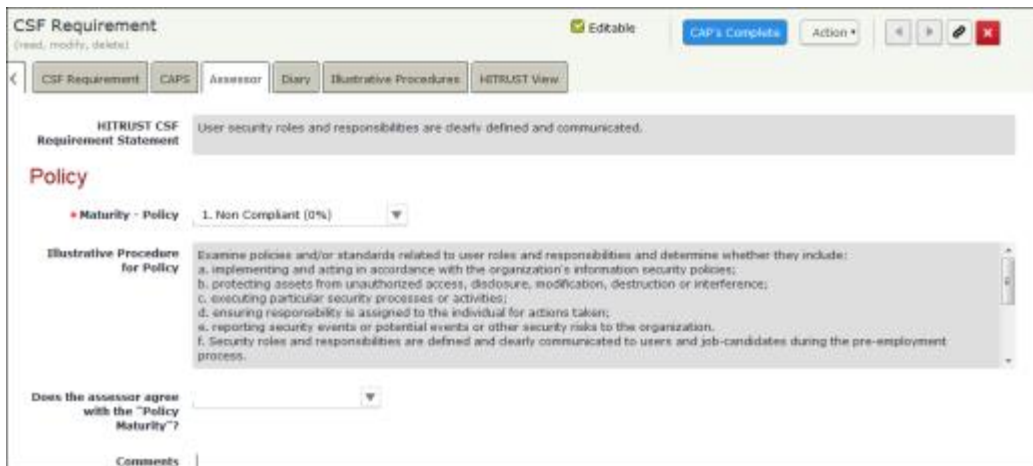
5. When the record opens, enter the values for fields listed in the following table:

Field	Value
Status of the Cap	Started - On track
Estimated Date of Completion	*Select a date the cap will be completed
Enter your CAP Step below	Re-define the Guest role
Enter Email address for cap recipient	*Select an email address of the recipients you want to notify about the cap. Make sure to click the Send Details to Recipient link.

**Enter values of your choice.*

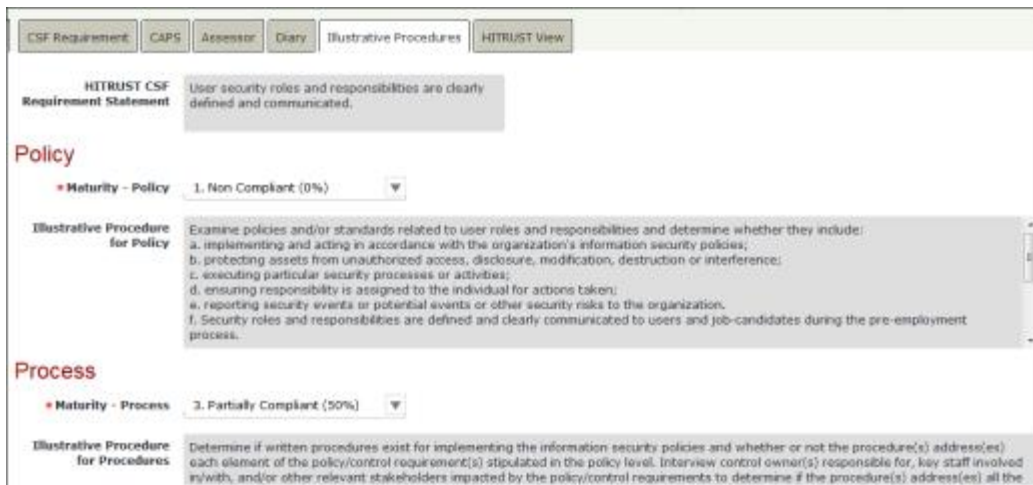


6. Click **Save & Close**.
7. Additional cap steps can be created, if desired. To create a new cap step, click **Add** and select **CSF Cap Steps**. In the **CSF Cap Steps (new)** form, complete all the required fields and click **Save & Close**.
8. Click the **Assessor** tab to validate your client's answers for each of the five maturity levels – Policy, Process, Implemented, Measured, and Managed. To validate the answers, you will need to examine supporting documentation, interview those responsible for the control, and perform relevant tests, where possible, to ensure that the control is operating as required.



The screenshot shows the 'CSF Requirement' form in the 'Assessor' tab. The 'HITRUST CSF Requirement Statement' is 'User security roles and responsibilities are clearly defined and communicated.' The 'Policy' maturity level is set to '1. Non Compliant (0%)'. The 'Illustrative Procedure for Policy' is 'Examine policies and/or standards related to user roles and responsibilities and determine whether they include: a. implementing and acting in accordance with the organization's information security policies; b. protecting assets from unauthorized access, disclosure, modification, destruction or interference; c. executing particular security processes or activities; d. ensuring responsibility is assigned to the individual for actions taken; e. reporting security events or potential events or other security risks to the organization; f. Security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.' The 'Does the assessor agree with the "Policy Maturity"?' field is empty. The 'Comments' field is also empty.

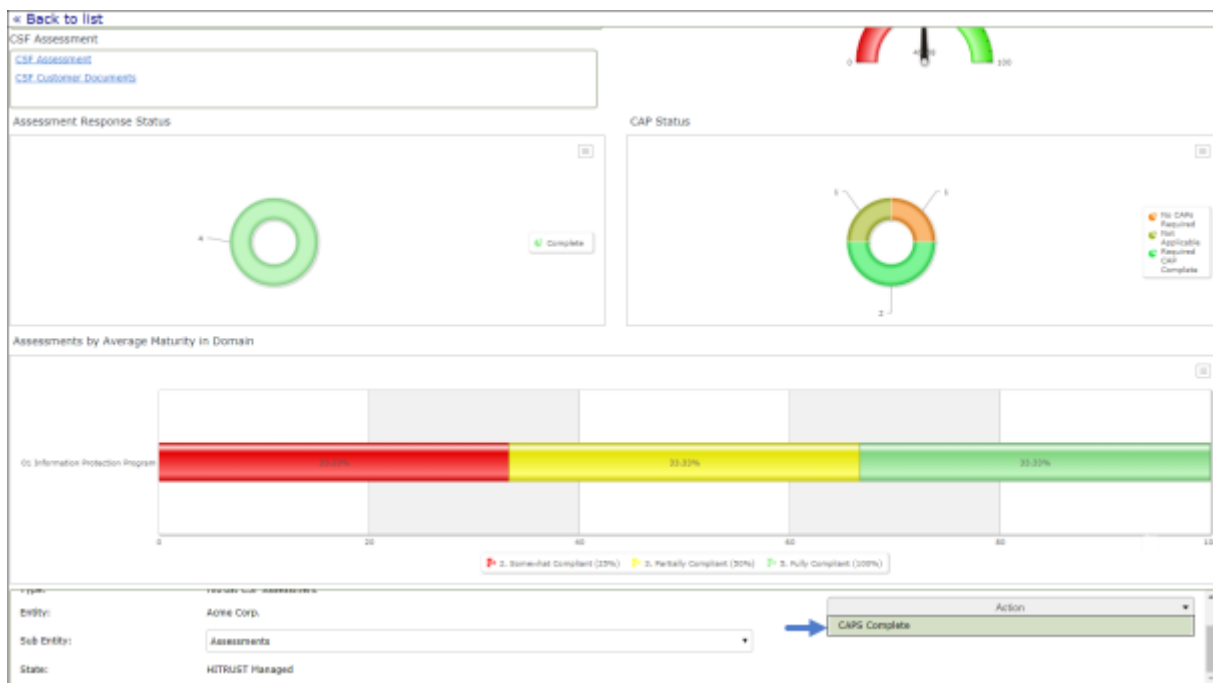
9. Click the **Illustrative Procedures** tab to determine the required actions or evidence for each maturity rating.



The screenshot shows the 'CSF Requirement' form in the 'Illustrative Procedures' tab. The 'HITRUST CSF Requirement Statement' is 'User security roles and responsibilities are clearly defined and communicated.' The 'Policy' maturity level is set to '1. Non Compliant (0%)'. The 'Illustrative Procedure for Policy' is 'Examine policies and/or standards related to user roles and responsibilities and determine whether they include: a. implementing and acting in accordance with the organization's information security policies; b. protecting assets from unauthorized access, disclosure, modification, destruction or interference; c. executing particular security processes or activities; d. ensuring responsibility is assigned to the individual for actions taken; e. reporting security events or potential events or other security risks to the organization; f. Security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.' The 'Process' maturity level is set to '3. Partially Compliant (50%)'. The 'Illustrative Procedure for Procedures' is 'Determine if written procedures exist for implementing the information security policies and whether or not the procedure(s) address(es) each element of the policy/control requirement(s) stipulated in the policy level. Interview control owner(s) responsible for, key staff involved in/with, and/or other relevant stakeholders impacted by the policy/control requirements to determine if the procedure(s) address(es) all the

10. If you have made any changes, be sure to click **Save & Close**.
11. Repeat steps 6 through 15 if there are more gaps in the domain.

12. Once you have completed all CAPs, the chart CAP Status will indicate Required CAPs Complete and you can click the object workflow button CAPs Complete.



Appendix 1: Email Notifications and Offline Decision Making

Setting up Email Addresses

This module is configured to send automated email notifications at specific points in the workflow. In a production box, email addresses are usually gathered automatically using an LDAP server or a directory service. However, the email addresses in your Rsam instance can be manually entered for testing purposes.

Procedure:

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the HITRUST MyCSF Module module.
2. Sign in as `r_admin` user. Enter **Username** as `r_admin` and **Password** as `password`.
3. Navigate to **Manage > Users/Groups**.
4. Double-click a user row to open the details.
5. Enter an email address in the **eMail ID** attribute.

The screenshot shows the 'User Details' form. It includes fields for 'User Id' (152048), 'First Name' (May), 'Middle Name' (empty), 'Last Name' (Brian), 'eMail ID' (support@rsam.com), 'Phone Number' (empty), 'Password' (masked with dots), and 'Confirm Password' (empty). There is a checkbox for 'LDAP User' which is currently unchecked. Below this, there is a section for 'User's LDAP ID' (empty) and 'User's LDAP Domain' (a dropdown menu showing 'Please select a Domain').

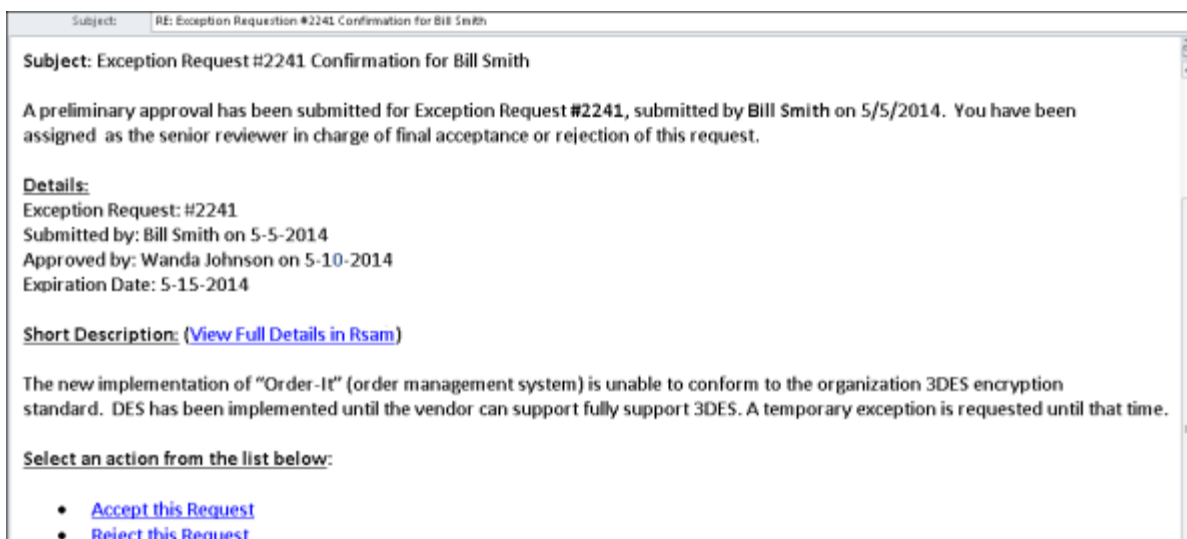
6. Click **OK**.

The email address of the user account is saved.

Offline Decision Making

Rsam email notifications are configurable including what notification should be sent, what users or roles will receive the notifications, and the content in the notifications. The following image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Rsam's Offline Decision Making.

Offline Decision Making is one of Rsam's powerful and popular features. It provides the Rsam platform directly to the users to perform workflow actions without connecting to the Rsam module.



Appendix 2: Rsam Documentation

HITRUST MyCSF Module Baseline Configuration Guide

To learn more about the pre-configurations in the HITRUST MyCSF Module, refer the HITRUST MyCSF Module Step-by-Step Tutorial. You should have received the HITRUST MyCSF Module Baseline Configuration Guide along with the HITRUST MyCSF Module sandbox. If not, please contact your Rsam Representative to obtain an electronic copy of the HITRUST MyCSF Module Baseline Configuration Guide.

Inline Help

This tutorial provides the step-by-step instructions on the Rsam HITRUST MyCSF Module. To get familiar with the specific Rsam features used in this configuration, refer the Rsam Help, Rsam Administrator Help, or both. The Online help you can access depends on your user permissions.

Procedure:

1. Sign in to your Rsam instance. For example, sign in as **Example Administrator** user. Enter **Username** as **r_admin** and **Password** as **password**.
2. Mouse hover over **Help** and select an Online help in the menu that appears. Depending on your user permissions, you will be able to access the Rsam Help, Rsam Administrator Help, or both.

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

