ISAAC 2013: Instructions for Laserfiche Repositories

The Information Security Awareness, Assessment and Compliance (ISAAC) season is officially underway for 2013, and it is time again to work on an assessment for your Laserfiche repository. All ISAAC reports must be completed by November 27. The 2013 ISAAC application has been updated to include special consideration for the Texas A&M IT Laserfiche Shared Service. Last year, you provided information from a data owner's perspective about the repository under your department or agency's control. The shared service then incorporated your responses into the online ISAAC report for the Laserfiche application.

This year, IT Risk Management has modified the ISAAC application to allow you to directly provide the information about your repository online.

The following screen captures present an overview of the Laserfiche repository resource for this ISAAC season. The screen captures are based on a sample CIS repository. Links to help material and training are available at https://isaac.tamu.edu/RA/help-main.cfm.

Keep in mind that for the assessment to be complete, the report must be printed, signed and the online ISAAC marked as completed/certified. Therefore, please leave additional time for those steps to be completed before the deadline.

This document has been prepared to assist Laserfiche Shared Services customers in navigating the first online ISAAC for your Laserfiche repository.

ISAAC

Getting started:

The steps to complete the online ISAAC for Laserfiche Repositories include:

1. Select Unit(s): Identify the units that own and use the information resources you are assessing.

2. Create Contacts: Create contact records for information resource owners, custodians and others who will sign the assessment.

3. Create Resources: Create records for the resources you are assessing, so you may select them when you create an assessment.

4. Perform Assessment: Select the resources to be assessed, answer questions and plan for remediation if necessary.

5. Print Report: Print an assessment for review and signature by appropriate individuals.

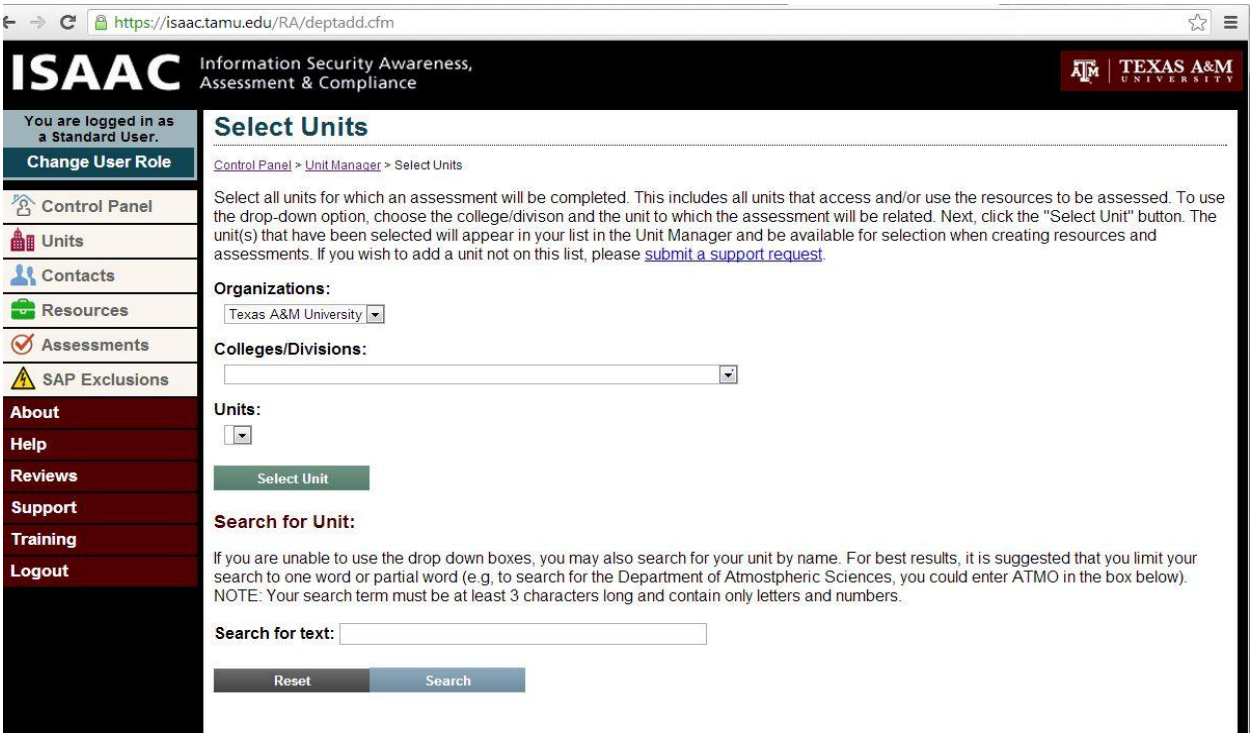
6. Mark Assessment Completed/Certified: Mark the assessment as completed and certified after obtaining necessary signatures.

The following text and screen captures present a step-by-step walkthrough using a example CIS repository.

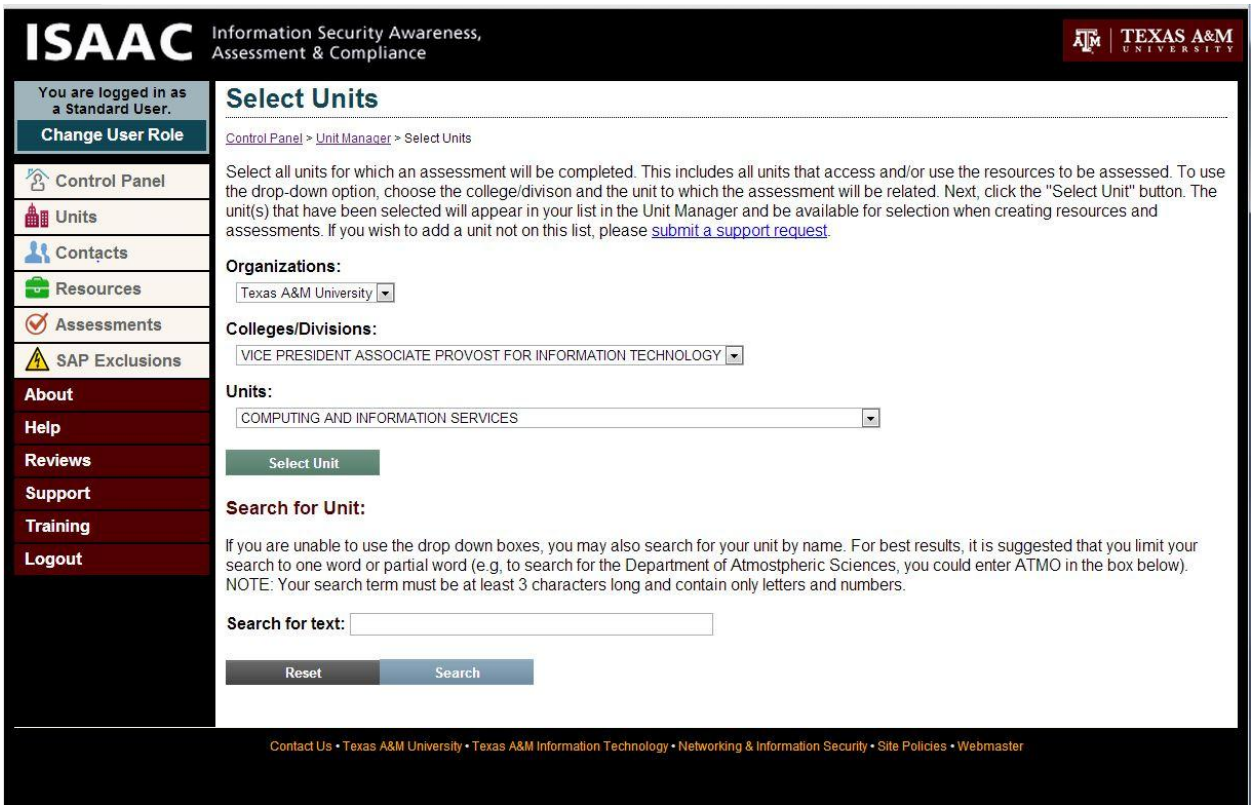
From the ISAAC home page (https://isaac.tamu.edu/RA/index.cfm), click the Login link and authenticate with your NetID and password. ISAAC creates your account automatically upon first login.

Step 1: Select Units

After logging in to ISAAC, select the “Path 2: Standard” role. Select Units from the left column.



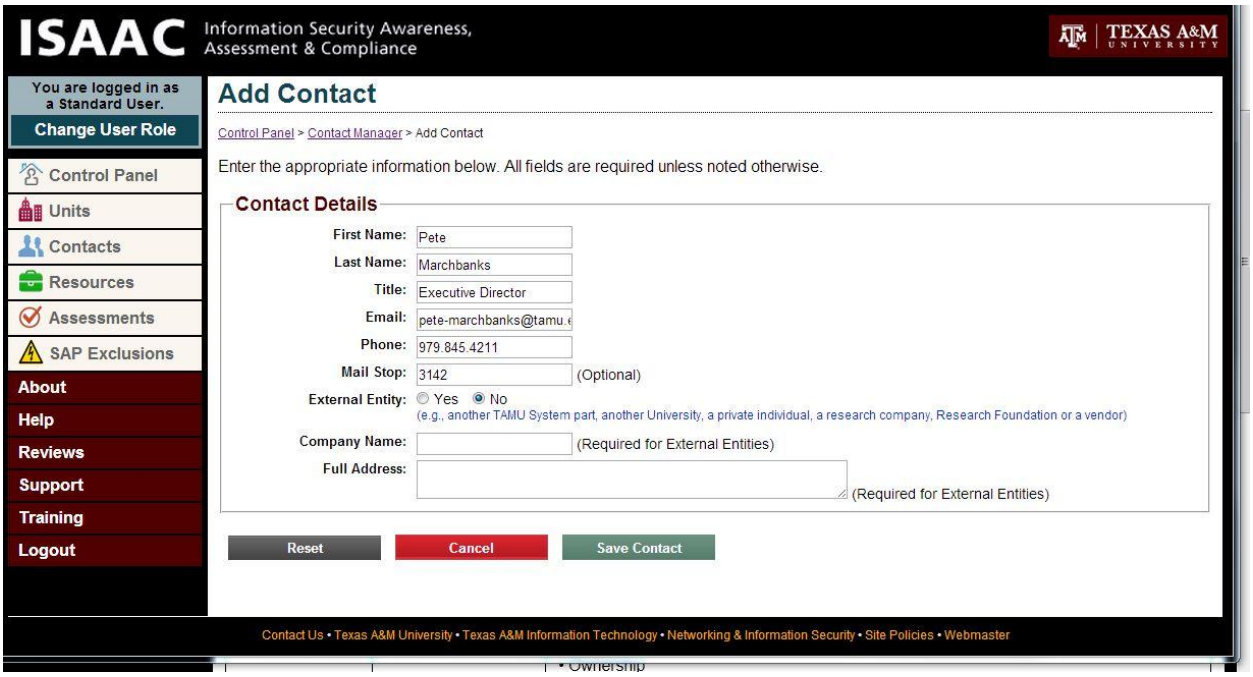
Identify your Organization, College/Division, and Unit from the dropdown boxes. In this example, the fields have been completed for Computing and information Services (CIS).



Step 2: Add contacts

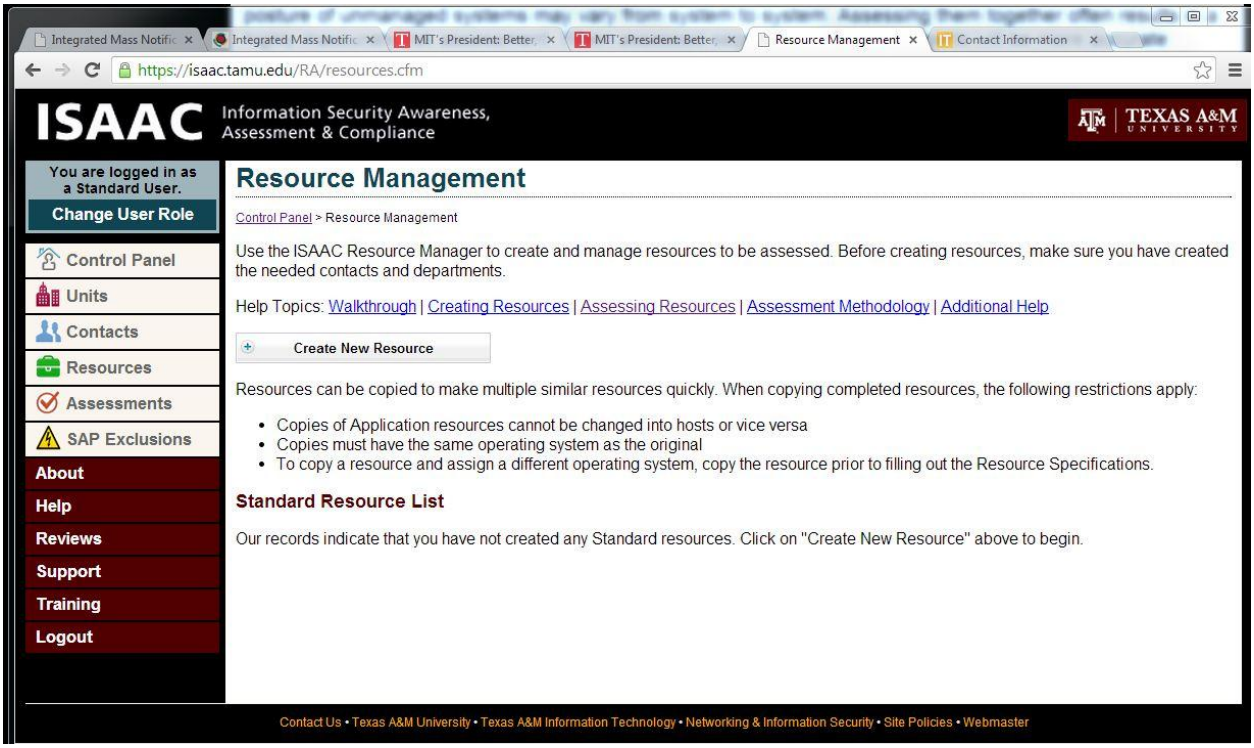
Select Contacts from the left column. Create contact information for the Resource owner, Resource custodian, and Department Head. If your group has an Information Security Administrator, create that contact.

In this example, Dr. Pete Marchbanks is both the Department Head and the Resource Owner for CIS' Business Services repository. Sophia Dunlap serves as the custodian for the CIS repository.



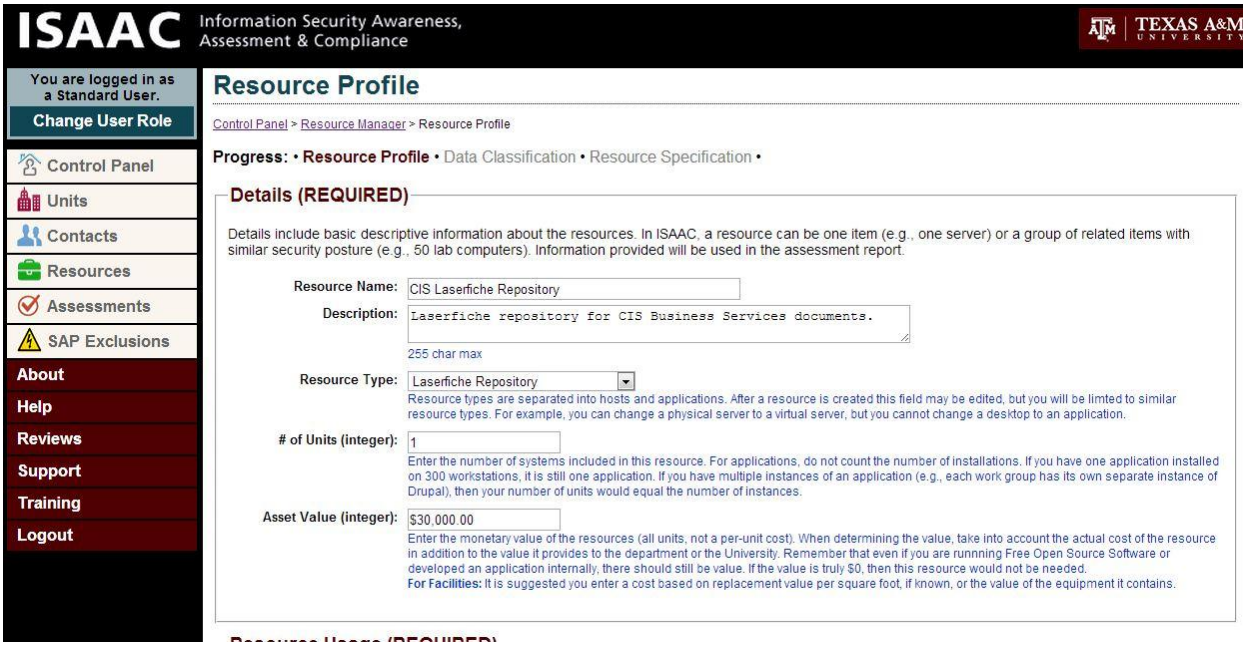
Step 3: Resource Management

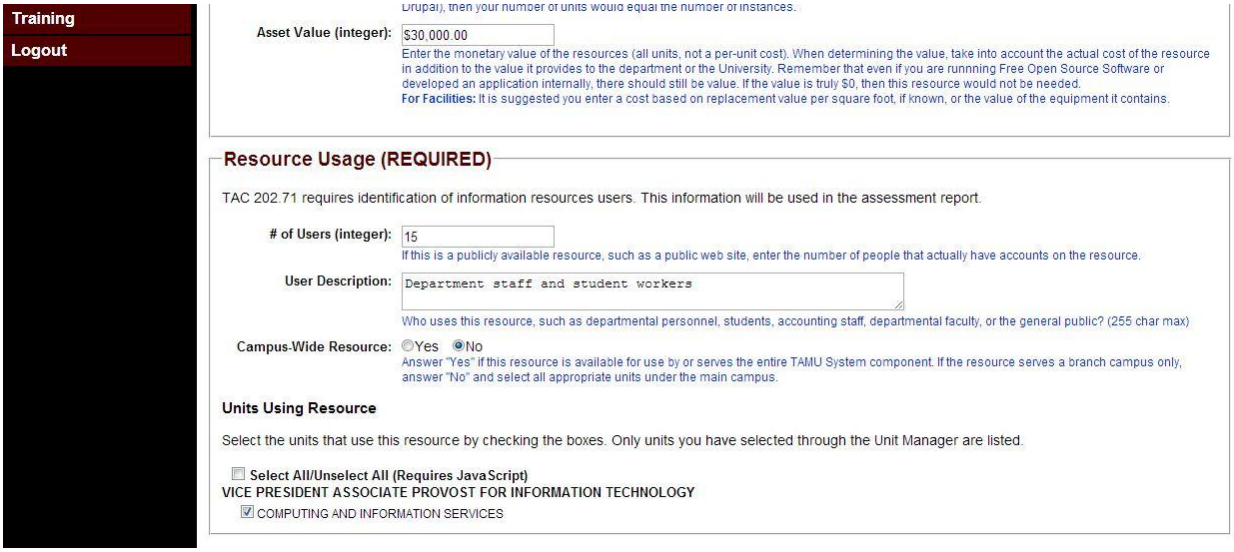
Select Resources from the left column. Click “Create New Resource.”



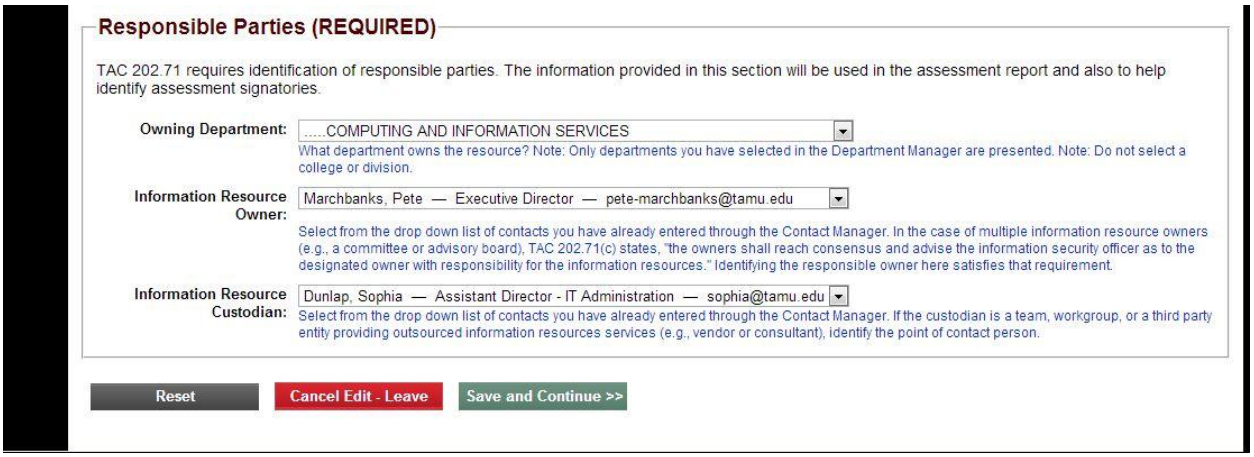
The Resource Profile page contains three sections. Complete each section of the Resource Profile.

Attached is an example of a completed Resource Profile. The number of units being reported for this resource should be one (1) in the case of a Laserfiche resource. If your department or agency controls more than one repository, a separate ISAAC assessment should be completed for each repository.



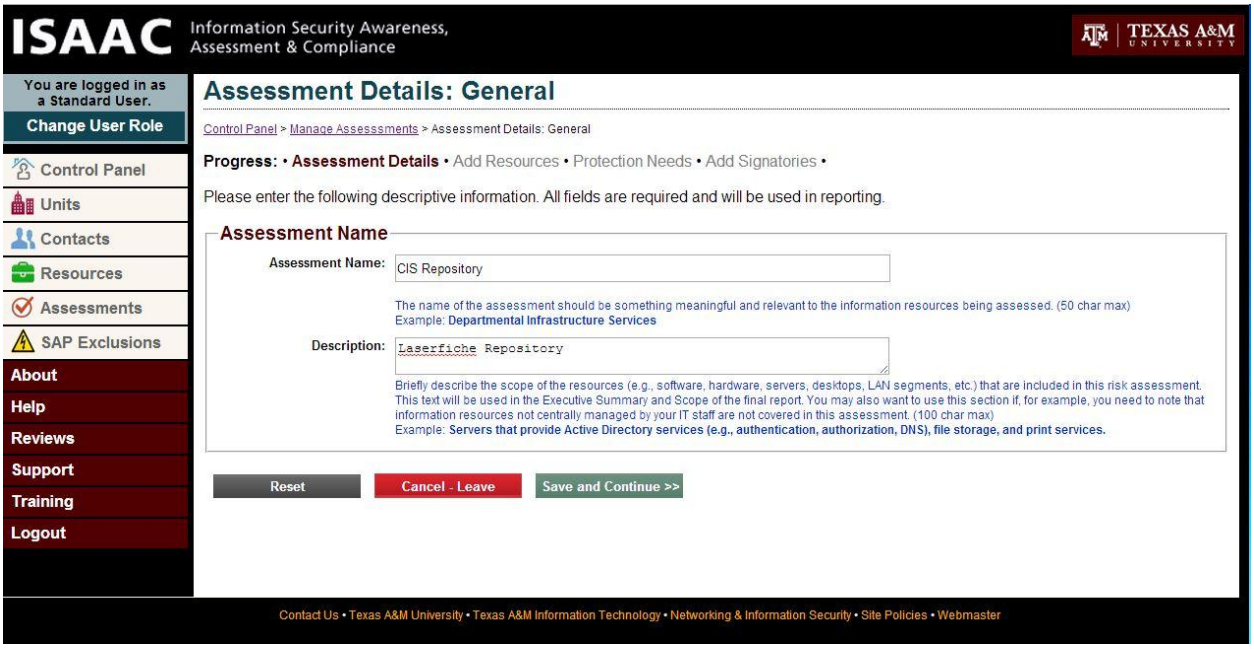


Select Department, Resource Owner and Resource Custodian from the dropdowns. These contacts were created in “Step 2: Create Contacts.”

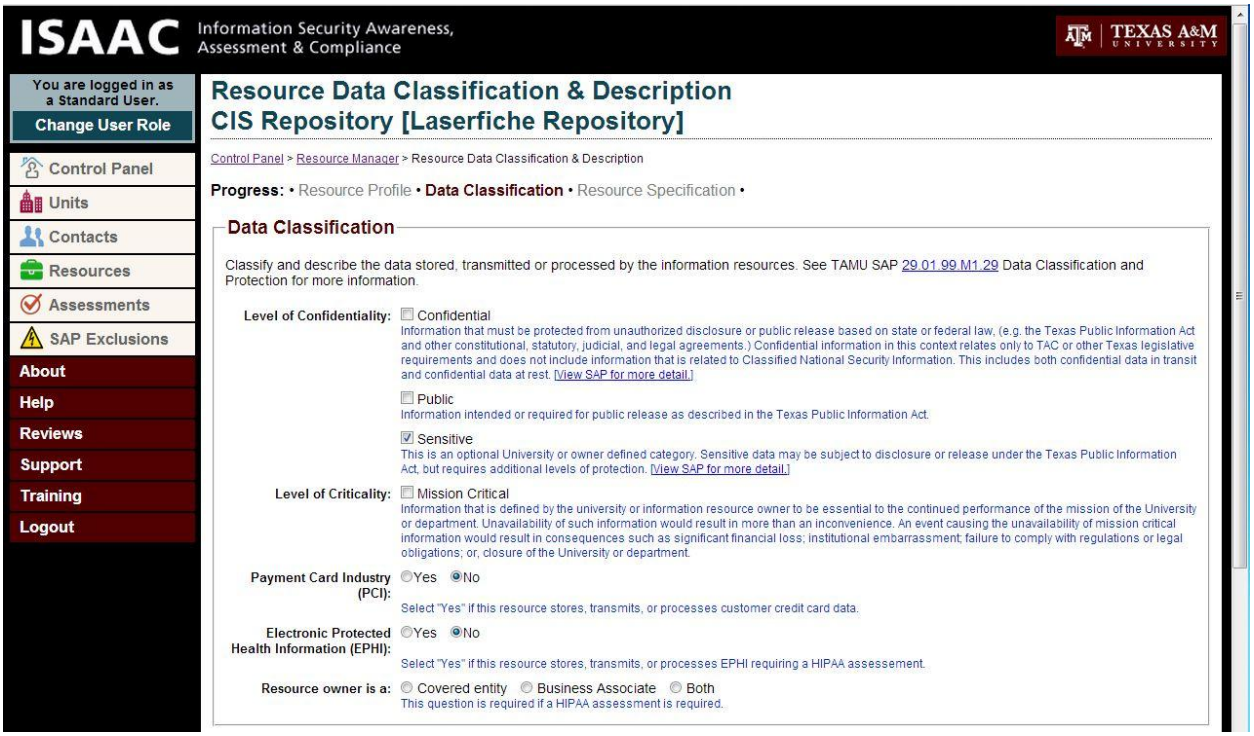


Step 4: Assessment Details

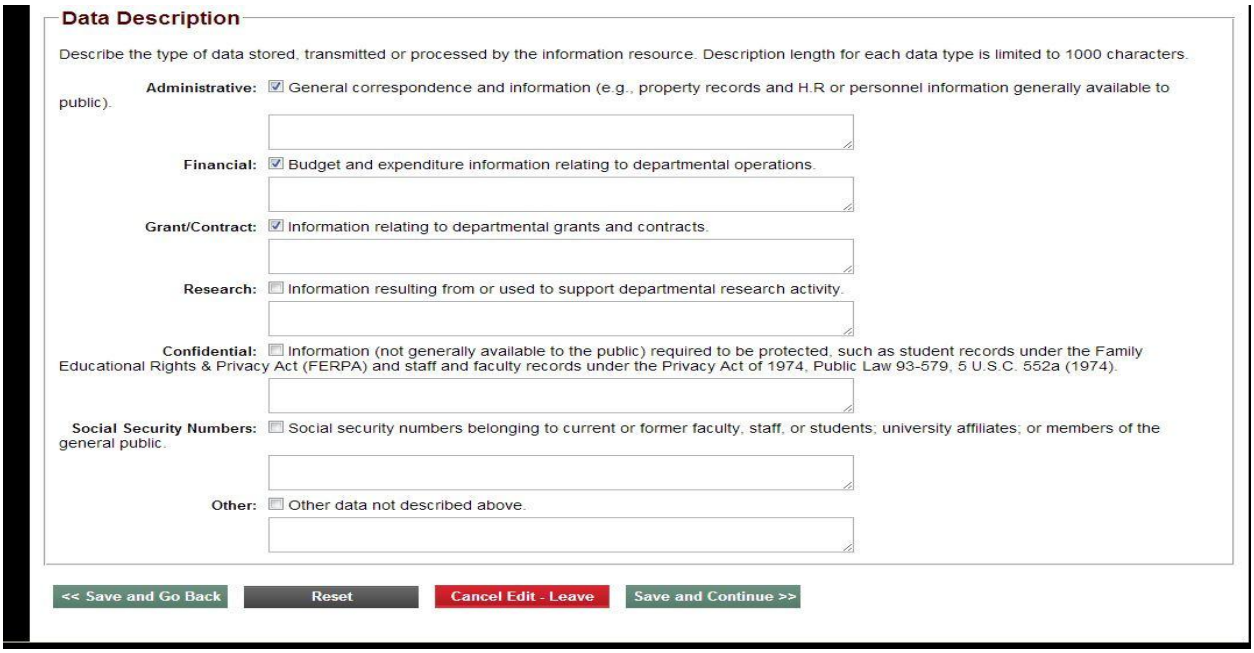
Enter descriptive information about the resource.



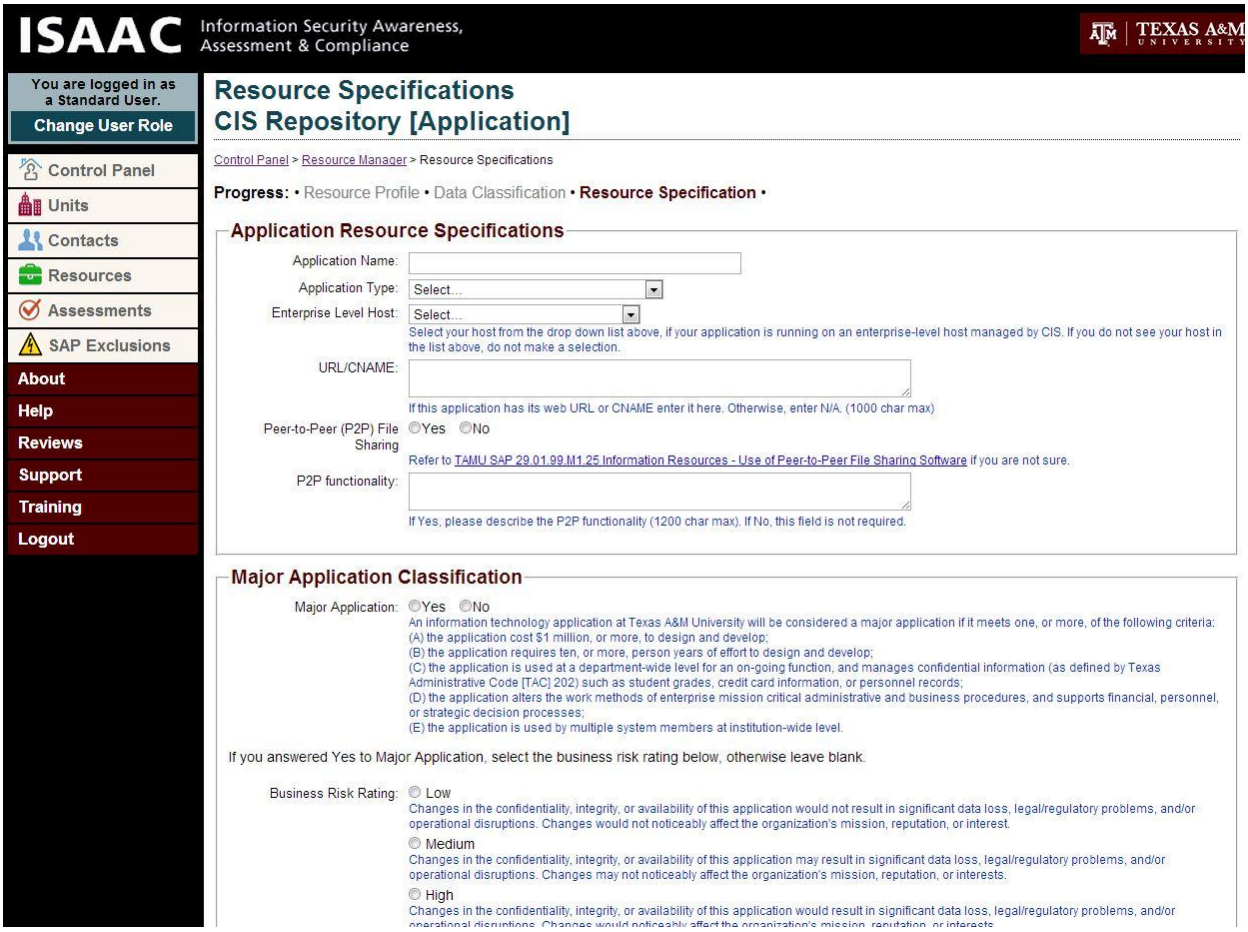
Choose the classification of the repository data.



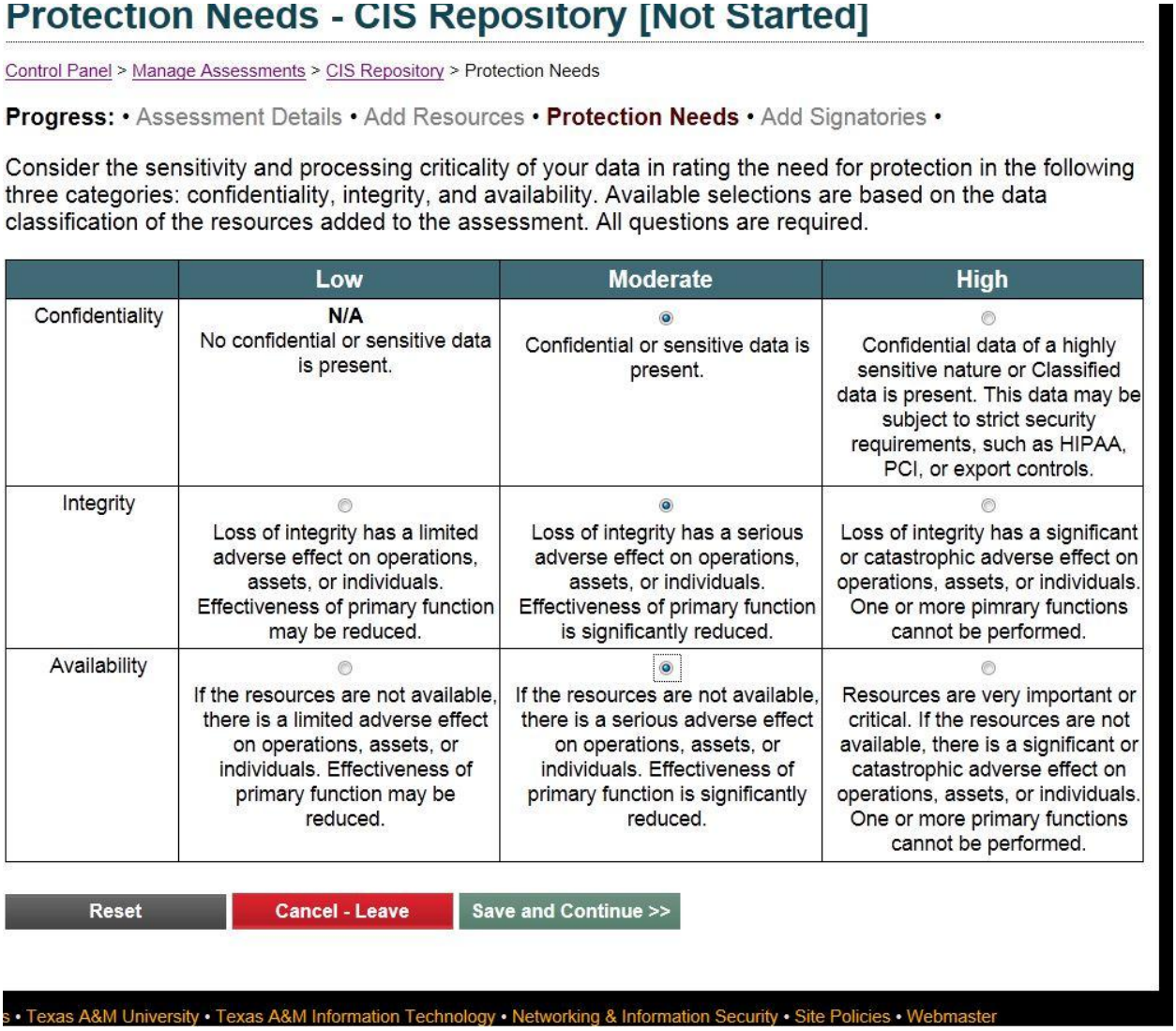
Provide a data description of the files processed and stored in your repository.



Document the resource specification and determine whether your use of the resource constitutes a major application based on the university's definition (SAP 29.01.99.M1.21 Information Resources). For Application Type, select "Purchased with Customization". For an Enterprise Level Host, select CIS Virtualization and Data Storage. The URL/CNAME can be left as N/A. Select "No" for P2P File Sharing. Determine the major application based on your use of the repository consistent with the university definition.



A screen entitled “Assessments without Resources” appears. Select “Continue Creating” under the Actions. The next screen lists the available resources. Look for the table under the heading “Add Application (Software application, File Stores, Data Repositories). Click the “Add” button next to the repository resource you created. Complete the Protection Needs page.



Protection Needs - CIS Repository [Not Started]

Control Panel > Manage Assessments > CIS Repository > Protection Needs

Progress: • Assessment Details • Add Resources • **Protection Needs** • Add Signatories •

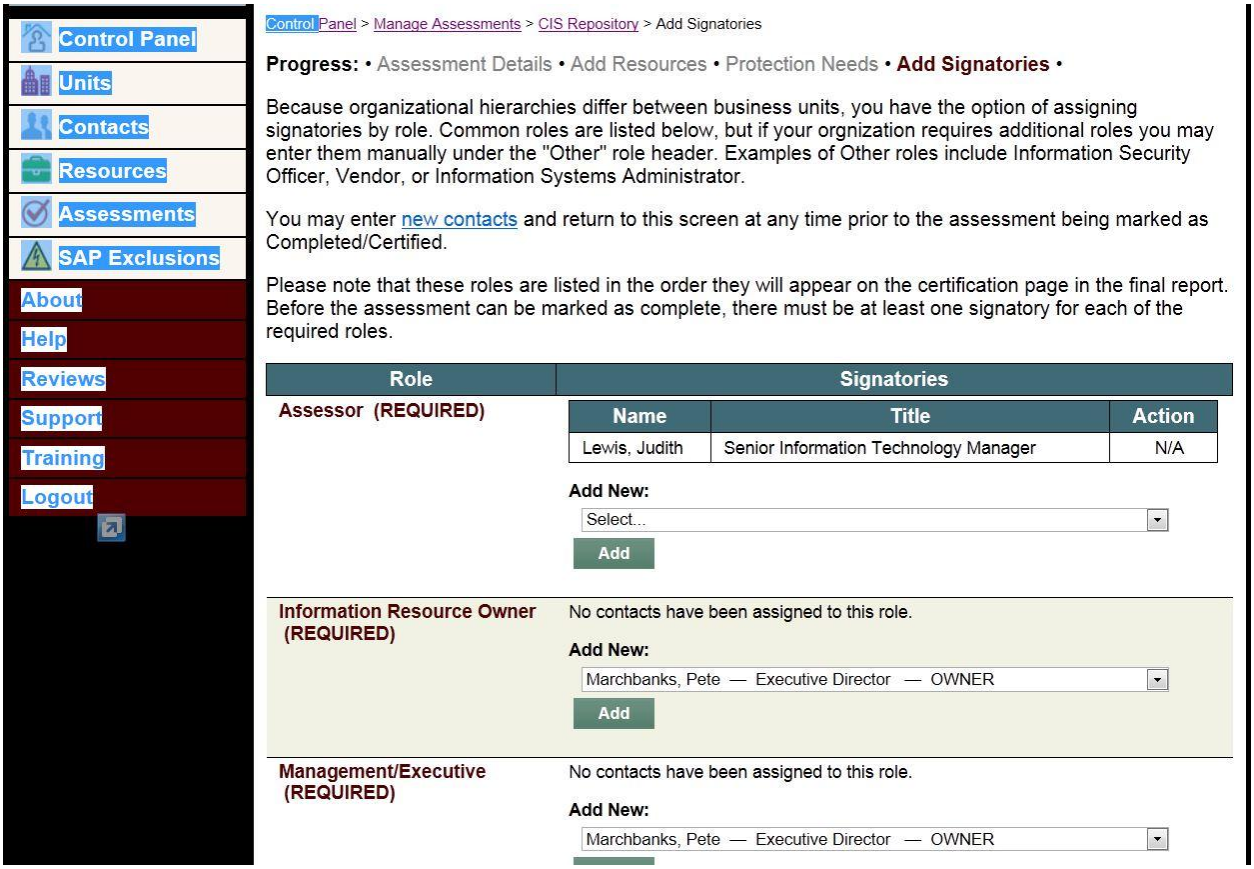
Consider the sensitivity and processing criticality of your data in rating the need for protection in the following three categories: confidentiality, integrity, and availability. Available selections are based on the data classification of the resources added to the assessment. All questions are required.

	Low	Moderate	High
Confidentiality	**N/A** No confidential or sensitive data is present.	◉ Confidential or sensitive data is present.	○ Confidential data of a highly sensitive nature or Classified data is present. This data may be subject to strict security requirements, such as HIPAA, PCI, or export controls.
Integrity	○ Loss of integrity has a limited adverse effect on operations, assets, or individuals. Effectiveness of primary function may be reduced.	◉ Loss of integrity has a serious adverse effect on operations, assets, or individuals. Effectiveness of primary function is significantly reduced.	○ Loss of integrity has a significant or catastrophic adverse effect on operations, assets, or individuals. One or more pimrary functions cannot be performed.
Availability	○ If the resources are not available, there is a limited adverse effect on operations, assets, or individuals. Effectiveness of primary function may be reduced.	◉ If the resources are not available, there is a serious adverse effect on operations, assets, or individuals. Effectiveness of primary function is significantly reduced.	○ Resources are very important or critical. If the resources are not available, there is a significant or catastrophic adverse effect on operations, assets, or individuals. One or more primary functions cannot be performed.

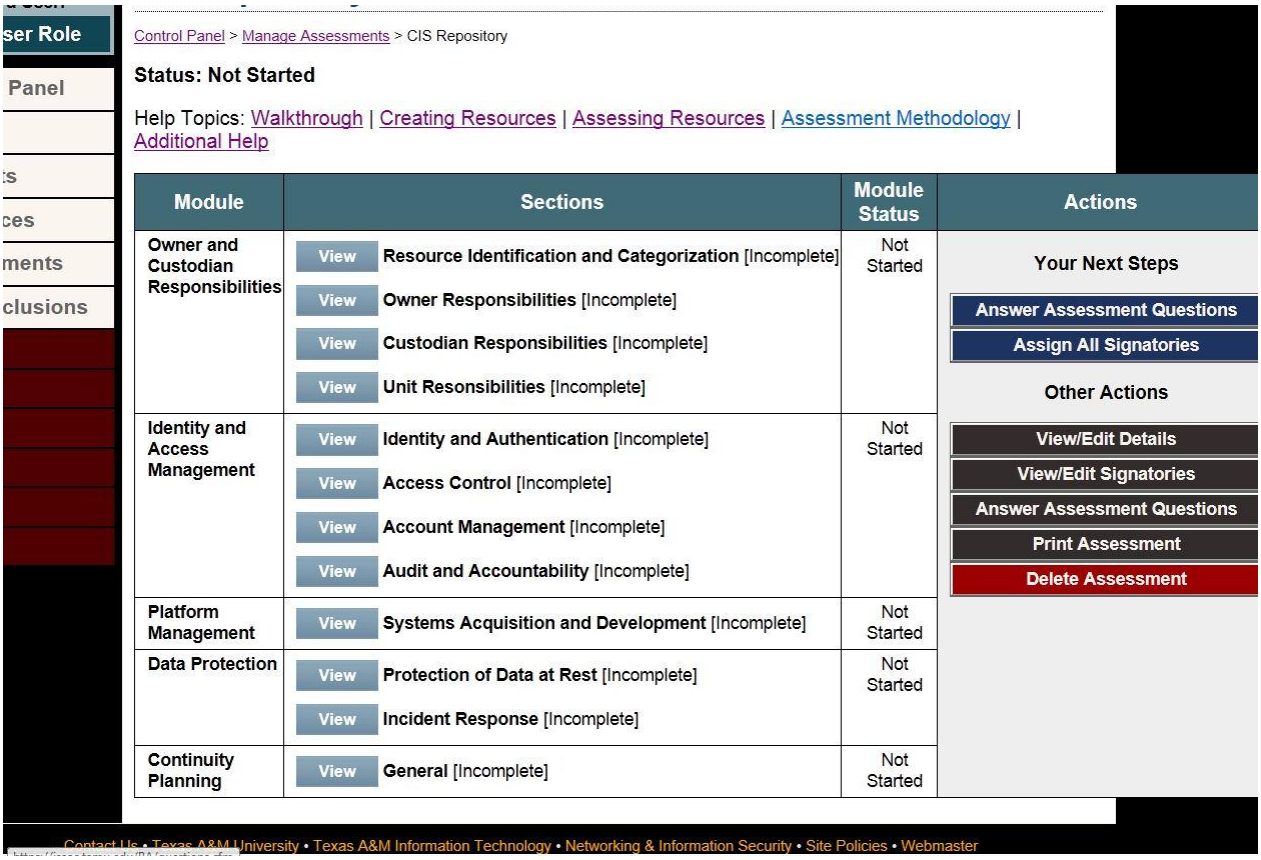
Reset | Cancel - Leave | Save and Continue >>

s • Texas A&M University • Texas A&M Information Technology • Networking & Information Security • Site Policies • Webmaster

Finally, assign signatory roles. Be sure click the “Add” button after making each selection.

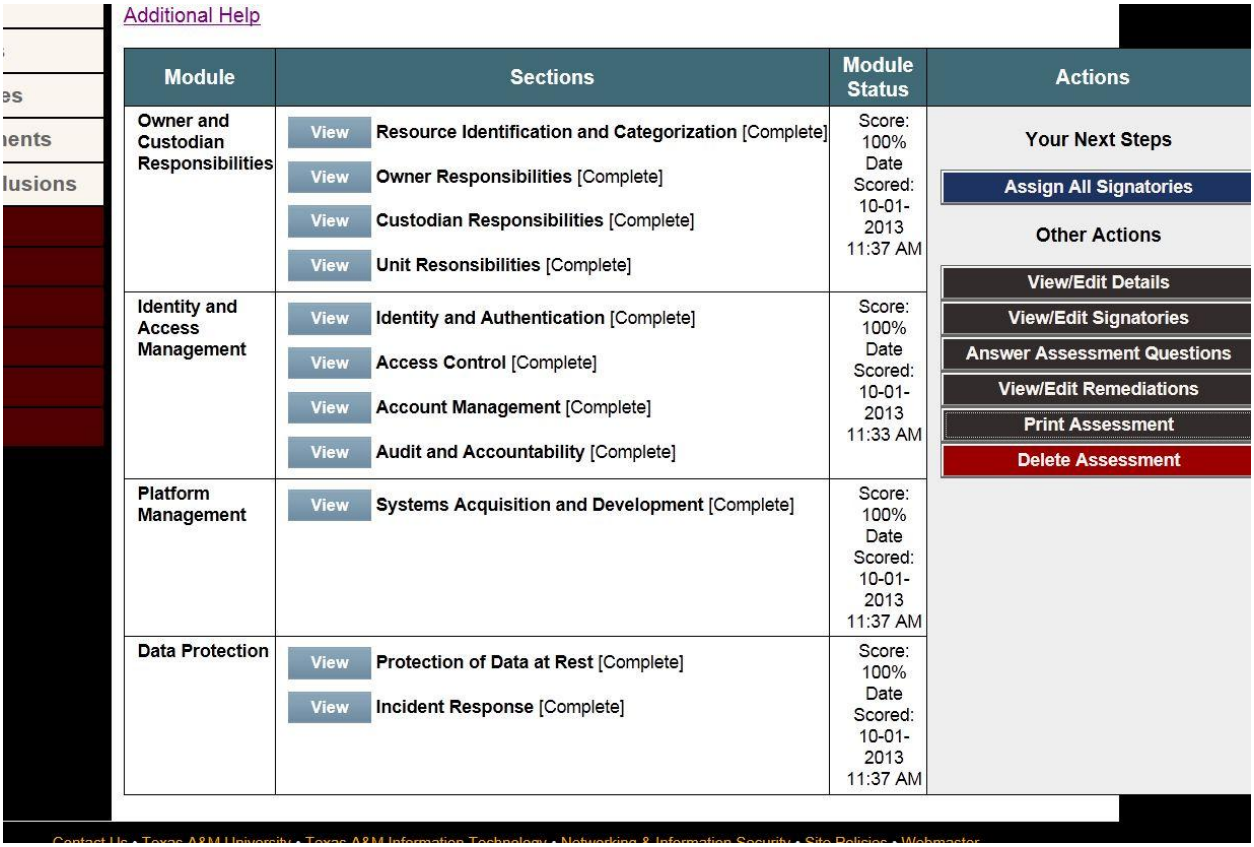


Next, the Module Status screen appears, which presents the assessments remaining as determined by the ISAAC methodology based on your answers to the preceding sections. This is an example of the status page.



Either view each section to answer the questions individually or select “Answer Assessment Questions”, answering each section and using the “Save and Continue” button to advance to the next section. After answering the Assessment questions for each module, view your ISAAC score by selecting the “Score Now” button.

This is an example of the scored assessment.



Step 5: Print Report

Print the assessment by selecting the "Print Assessment" button on the Assessment Methodology page.

Maintain a signed copy of your ISAAC report for use if that risk assessment is selected for review next year or if your department gets audited. See records retention requirements to see how long reports must be kept.

Step 6: Mark Assessment completed/Certified

After the report is signed, return to ISAAC and mark the assessment as Completed/Certified on the Open Assessment screen. This is the final step and needs to be performed online to complete the ISAAC assessment. The information resources in the assessment have not been officially assessed and reported, until this has been done.

If you have additional ISAAC questions, contact ISAAC technical support by emailing isaac-support@tamu.edu. If you need immediate assistance, call IT Risk Management at 979.845.9254.