

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.

The screenshot shows the ISAAC web interface. The top navigation bar includes links for Control Panel, Unit Manager, and Select Units. The main content area is titled "Select Units" and displays instructions for selecting units for assessment. It features dropdown menus for "Organizations" (set to Texas A&M University) and "Colleges/Divisions" (a dropdown menu). Below these are dropdown menus for "Units" and a "Select Unit" button. A search section titled "Search for Unit" includes a text input field and a "Search" button. On the far left, a vertical sidebar lists navigation links: Control Panel, Units, Contacts, Resources, Assessments, SAP Exclusions, About, Help, Reviews, Support, Training, and Logout. The "Assessments" link is highlighted with a red background.

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).

ISAAC Information Security Awareness, Assessment & Compliance

You are logged in as a Standard User.

[Change User Role](#)

[!\[\]\(4222901cb0b23d3b20e48e0aa550c263_img.jpg\) Control Panel](#)

[!\[\]\(35de7ce9c97e259aff6f01ac90da87f8_img.jpg\) Units](#)

[!\[\]\(62d4d3494d4340f830d2a84926a2cbde_img.jpg\) Contacts](#)

[!\[\]\(f352fb86fd942855f49bb0ef3403ffdf_img.jpg\) Resources](#)

[!\[\]\(bb7d30538f2dfd629b893033401c9a1c_img.jpg\) Assessments](#)

[!\[\]\(62858d4247555be7beae258ecdaf2710_img.jpg\) SAP Exclusions](#)

[About](#)

[Help](#)

[Reviews](#)

[Support](#)

[Training](#)

[Logout](#)

Select Units

[Control Panel](#) > [Unit Manager](#) > Select Units

Select all units for which an assessment will be completed. This includes all units that access and/or use the resources to be assessed. To use the drop-down option, choose the college/division and the unit to which the assessment will be related. Next, click the "Select Unit" button. The unit(s) that have been selected will appear in your list in the Unit Manager and be available for selection when creating resources and assessments. If you wish to add a unit not on this list, please [submit a support request](#).

Organizations:

Colleges/Divisions:

Units:

[Select Unit](#)

Search for Unit:

If you are unable to use the drop down boxes, you may also search for your unit by name. For best results, it is suggested that you limit your search to one word or partial word (e.g., to search for the Department of Atmospheric Sciences, you could enter ATMO in the box below).
NOTE: Your search term must be at least 3 characters long and contain only letters and numbers.

Search for text:

[Reset](#) [Search](#)

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

 TEXAS A&M UNIVERSITY

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.

The screenshot shows the ISAAC Control Panel interface. On the left is a vertical sidebar with links: Control Panel, Units, Contacts, Resources, Assessments (highlighted with a red checkmark), SAP Exclusions, About, Help, Reviews, Support, Training, and Logout. The main content area has a header "Add Contact" and a breadcrumb trail "Control Panel > Contact Manager > Add Contact". A message says "Enter the appropriate information below. All fields are required unless noted otherwise." The "Contact Details" form contains the following data:

First Name:	Pete
Last Name:	Marchbanks
Title:	Executive Director
Email:	pete-marchbanks@tamu.edu
Phone:	979.845.4211
Mail Stop:	3142
External Entity:	<input type="radio"/> Yes <input checked="" type="radio"/> No (e.g., another TAMU System part, another University, a private individual, a research company, Research Foundation or a vendor)
Company Name:	[empty]
Full Address:	[empty]

At the bottom are three buttons: Reset, Cancel, and Save Contact (highlighted in green).

At the very bottom of the page, there is a footer bar with links: Contact Us • Texas A&M University • Texas A&M Information Technology • Networking & Information Security • Site Policies • Webmaster.

Step 3: Resource Management

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

The screenshot shows a web browser window with the URL <https://isaac.tamu.edu/RA/resources.cfm>. The page is titled "Resource Management". On the left, there is a vertical navigation menu with the following items: Control Panel, Units, Contacts, Resources, Assessments (which is checked), SAP Exclusions, About, Help, Reviews, Support, Training, and Logout. A message at the top of the menu says "You are logged in as a Standard User." Below the menu, the main content area has a heading "Resource Management" and a breadcrumb trail "Control Panel > Resource Management". It contains instructions for using the ISAAC Resource Manager to create and manage resources, mentioning the need to create contacts and departments before creating resources. It also lists help topics: Walkthrough, Creating Resources, Assessing Resources, Assessment Methodology, and Additional Help. A prominent button labeled "Create New Resource" is visible. Below this, a section titled "Standard Resource List" states that no resources have been created yet and provides a link to begin. At the bottom of the page, there is a footer with links to Contact Us, Texas A&M University, Texas A&M Information Technology, Networking & Information Security, Site Policies, and Webmaster.

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.

You are logged in as
a Standard User.[Change User Role](#)[Units](#)[Contacts](#)[Resources](#)[Assessments](#)[SAP Exclusions](#)[About](#)[Help](#)[Reviews](#)[Support](#)[Training](#)[Logout](#)

Resource Profile

[Control Panel](#) > [Resource Manager](#) > Resource ProfileProgress: • **Resource Profile** • Data Classification • Resource Specification •

Details (REQUIRED)

Details include basic descriptive information about the resources. In ISAAC, a resource can be one item (e.g., one server) or a group of related items with similar security posture (e.g., 50 lab computers). Information provided will be used in the assessment report.

Resource Name: Description:
255 char maxResource Type:

Resource types are separated into hosts and applications. After a resource is created this field may be edited, but you will be limited to similar resource types. For example, you can change a physical server to a virtual server, but you cannot change a desktop to an application.

of Units (integer):

Enter the number of systems included in this resource. For applications, do not count the number of installations. If you have one application installed on 300 workstations, it is still one application. If you have multiple instances of an application (e.g., each work group has its own separate instance of Drupal), then your number of units would equal the number of instances.

Asset Value (integer):

Enter the monetary value of the resources (all units, not a per-unit cost). When determining the value, take into account the actual cost of the resource in addition to the value it provides to the department or the University. Remember that even if you are running Free Open Source Software or developed an application internally, there should still be value. If the value is truly \$0, then this resource would not be needed.

For Facilities: It is suggested you enter a cost based on replacement value per square foot, if known, or the value of the equipment it contains.

Resource Usage (REQUIRED)

Resource Usage (REQUIRED)

TAC 202.71 requires identification of information resources users. This information will be used in the assessment report.

of Users (integer):

If this is a publicly available resource, such as a public web site, enter the number of people that actually have accounts on the resource.

User Description:

Who uses this resource, such as departmental personnel, students, accounting staff, departmental faculty, or the general public? (255 char max)

Campus-Wide Resource: Yes No

Answer "Yes" if this resource is available for use by or serves the entire TAMU System component. If the resource serves a branch campus only, answer "No" and select all appropriate units under the main campus.

Units Using Resource

Select the units that use this resource by checking the boxes. Only units you have selected through the Unit Manager are listed.

 Select All/Unselect All (Requires JavaScript)

VICE PRESIDENT ASSOCIATE PROVOST FOR INFORMATION TECHNOLOGY

 COMPUTING AND INFORMATION SERVICES

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

Responsible Parties (REQUIRED)

TAC 202.71 requires identification of responsible parties. The information provided in this section will be used in the assessment report and also to help identify assessment signatories.

Owning Department:

What department owns the resource? Note: Only departments you have selected in the Department Manager are presented. Note: Do not select a college or division.

Information Resource Owner:

Select from the drop down list of contacts you have already entered through the Contact Manager. In the case of multiple information resource owners (e.g., a committee or advisory board), TAC 202.71(c) states, "the owners shall reach consensus and advise the information security officer as to the designated owner with responsibility for the information resources." Identifying the responsible owner here satisfies that requirement.

Information Resource Custodian:

Select from the drop down list of contacts you have already entered through the Contact Manager. If the custodian is a team, workgroup, or a third party entity providing outsourced information resources services (e.g., vendor or consultant), identify the point of contact person.

Step 4: Assessment Details

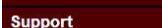
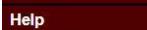
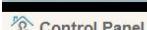
Enter descriptive information about the resource.



Information Security Awareness,
Assessment & Compliance



You are logged in as
a Standard User.



Assessment Details: General

[Control Panel](#) > [Manage Assessments](#) > [Assessment Details: General](#)

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

Please enter the following descriptive information. All fields are required and will be used in reporting.

Assessment Name

Assessment Name:

The name of the assessment should be something meaningful and relevant to the information resources being assessed. (50 char max)
Example: Departmental Infrastructure Services

Description:

Briefly describe the scope of the resources (e.g., software, hardware, servers, desktops, LAN segments, etc.) that are included in this risk assessment. This text will be used in the Executive Summary and Scope of the final report. You may also want to use this section if, for example, you need to note that information resources not centrally managed by your IT staff are not covered in this assessment. (100 char max)
Example: Servers that provide Active Directory services (e.g., authentication, authorization, DNS), file storage, and print services.

Choose the classification of the repository data.

You are logged in as a Standard User. [Change User Role](#)

Control Panel **Units** **Contacts** **Resources** **Assessments** **SAP Exclusions** **About** **Help** **Reviews** **Support** **Training** **Logout**

Resource Data Classification & Description CIS Repository [Laserfiche Repository]

Control Panel > Resource Manager > Resource Data Classification & Description

Progress: • Resource Profile • **Data Classification** • Resource Specification •

Data Classification

Classify and describe the data stored, transmitted or processed by the information resources. See TAMU SAP [29.01.99.M1.29](#) Data Classification and Protection for more information.

Level of Confidentiality: Confidential
Information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements.) Confidential information in this context relates only to TAC or other Texas legislative requirements and does not include information that is related to Classified National Security Information. This includes both confidential data in transit and confidential data at rest. [View SAP for more detail.](#)

Public
Information intended or required for public release as described in the Texas Public Information Act.

Sensitive
This is an optional University or owner defined category. Sensitive data may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection. [View SAP for more detail.](#)

Level of Criticality: Mission Critical
Information that is defined by the university or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss; institutional embarrassment; failure to comply with regulations or legal obligations; or, closure of the University or department.

Payment Card Industry (PCI): Yes No
Select "Yes" if this resource stores, transmits, or processes customer credit card data.

Electronic Protected Health Information (EPHI): Yes No
Select "Yes" if this resource stores, transmits, or processes EPHI requiring a HIPAA assessment.

Resource owner is a: Covered entity Business Associate Both
This question is required if a HIPAA assessment is required.

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

Data Description

Describe the type of data stored, transmitted or processed by the information resource. Description length for each data type is limited to 1000 characters.

Administrative: General correspondence and information (e.g., property records and H.R or personnel information generally available to public).

Financial: Budget and expenditure information relating to departmental operations.

Grant/Contract: Information relating to departmental grants and contracts.

Research: Information resulting from or used to support departmental research activity.

Confidential: Information (not generally available to the public) required to be protected, such as student records under the Family Educational Rights & Privacy Act (FERPA) and staff and faculty records under the Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a (1974).

Social Security Numbers: Social security numbers belonging to current or former faculty, staff, or students; university affiliates; or members of the general public.

Other: Other data not described above.

[<< Save and Go Back](#) [Reset](#) [Cancel Edit - Leave](#) [Save and Continue >>](#)

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.

ISAAC Information Security Awareness,
Assessment & Compliance

You are logged in as a Standard User.

[Change User Role](#)

- [Control Panel](#)
- [Units](#)
- [Contacts](#)
- [Resources](#)
- [Assessments](#)
- [SAP Exclusions](#)
- [**About**](#)
- [**Help**](#)
- [**Reviews**](#)
- [**Support**](#)
- [**Training**](#)
- [**Logout**](#)

Resource Specifications

CIS Repository [Application]

Control Panel > Resource Manager > Resource Specifications

Progress: • Resource Profile • Data Classification • **Resource Specification** •

Application Resource Specifications

Application Name:

 Application Type:

 Enterprise Level Host:
 Select your host from the drop down list above, if your application is running on an enterprise-level host managed by CIS. If you do not see your host in the list above, do not make a selection.

URL/CNAME:
 If this application has its web URL or CNAME enter it here. Otherwise, enter N/A. (1000 char max)

Peer-to-Peer (P2P) File Sharing: Yes No
 Refer to [TAMU SAP 29.01.99.M1.25 Information Resources - Use of Peer-to-Peer File Sharing Software](#) if you are not sure.

P2P functionality:
 If Yes, please describe the P2P functionality (1200 char max). If No, this field is not required.

Major Application Classification

Major Application: Yes No
 An information technology application at Texas A&M University will be considered a major application if it meets one, or more, of the following criteria:
 (A) the application cost \$1 million, or more, to design and develop;
 (B) the application requires ten or more, person years of effort to design and develop;
 (C) the application is used at a department-wide level for an on-going function, and manages confidential information (as defined by Texas Administrative Code [TAC] 202) such as student grades, credit card information, or personnel records;
 (D) the application alters the work methods of enterprise mission critical administrative and business procedures, and supports financial, personnel, or strategic decision processes;
 (E) the application is used by multiple system members at institution-wide level.

If you answered Yes to Major Application, select the business risk rating below, otherwise leave blank.

Business Risk Rating: Low
 Changes in the confidentiality, integrity, or availability of this application would not result in significant data loss, legal/regulatory problems, and/or operational disruptions. Changes would not noticeably affect the organization's mission, reputation, or interests.

Medium
 Changes in the confidentiality, integrity, or availability of this application may result in significant data loss, legal/regulatory problems, and/or operational disruptions. Changes may not noticeably affect the organization's mission, reputation, or interests.

High
 Changes in the confidentiality, integrity, or availability of this application would result in significant data loss, legal/regulatory problems, and/or operational disruptions. Changes would noticeably affect the organization's mission, reputation, or interests.

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	<input type="radio"/> N/A No confidential or sensitive data is present.	<input checked="" type="radio"/> Confidential or sensitive data is present.	<input checked="" type="radio"/> 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	<input checked="" type="radio"/> Loss of integrity has a limited adverse effect on operations, assets, or individuals. Effectiveness of primary function may be reduced.	<input checked="" type="radio"/> Loss of integrity has a serious adverse effect on operations, assets, or individuals. Effectiveness of primary function is significantly reduced.	<input checked="" type="radio"/> Loss of integrity has a significant or catastrophic adverse effect on operations, assets, or individuals. One or more primary functions cannot be performed.
Availability	<input checked="" type="radio"/> If the resources are not available, there is a limited adverse effect on operations, assets, or individuals. Effectiveness of primary function may be reduced.	<input checked="" type="radio"/> If the resources are not available, there is a serious adverse effect on operations, assets, or individuals. Effectiveness of primary function is significantly reduced.	<input checked="" type="radio"/> 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 >>](#)

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

Control Panel > Manage Assessments > CIS Repository > Add Signatories

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

Because organizational hierarchies differ between business units, you have the option of assigning signatories by role. Common roles are listed below, but if your organization requires additional roles you may enter them manually under the "Other" role header. Examples of Other roles include Information Security Officer, Vendor, or Information Systems Administrator.

You may enter [new contacts](#) and return to this screen at any time prior to the assessment being marked as Completed/Certified.

Please note that these roles are listed in the order they will appear on the certification page in the final report. Before the assessment can be marked as complete, there must be at least one signatory for each of the required roles.

Role	Signatories		
Assessor (REQUIRED)	Name	Title	Action
	Lewis, Judith	Senior Information Technology Manager	N/A

Add New:

Select...

Add

Information Resource Owner (REQUIRED) No contacts have been assigned to this role.

Add New:

Marchbanks, Pete — Executive Director — OWNER

Add

Management/Executive (REQUIRED) No contacts have been assigned to this role.

Add New:

Marchbanks, Pete — Executive Director — OWNER

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.

The screenshot shows a web-based application interface for managing assessments. On the left, there is a vertical sidebar with a dark background and light-colored text, listing categories like 'User Role', 'Panel', 'Assessments', and 'Conclusions'. The main content area has a header with the URL 'Control Panel > Manage Assessments > CIS Repository' and a status message 'Status: Not Started'. Below this, there are help topics and a table of modules and their sections. The table has columns for 'Module', 'Sections', 'Module Status', and 'Actions'. The 'Actions' column contains buttons for 'Your Next Steps' (Answer Assessment Questions, Assign All Signatories), 'Other Actions' (View/Edit Details, View/Edit Signatures, Answer Assessment Questions, Print Assessment, Delete Assessment), and a large red 'Delete Assessment' button. At the bottom of the page, there is a footer with a link to 'Contact Us' and other university resources.

Module	Sections	Module Status	Actions
Owner and Custodian Responsibilities	View Resource Identification and Categorization [Incomplete]	Not Started	Your Next Steps Answer Assessment Questions Assign All Signatories Other Actions View/Edit Details View/Edit Signatures Answer Assessment Questions Print Assessment Delete Assessment
	View Owner Responsibilities [Incomplete]		
	View Custodian Responsibilities [Incomplete]		
	View Unit Responsibilities [Incomplete]		
Identity and Access Management	View Identity and Authentication [Incomplete]		
	View Access Control [Incomplete]		
	View Account Management [Incomplete]		
	View Audit and Accountability [Incomplete]		
Platform Management	View Systems Acquisition and Development [Incomplete]	Not Started	
Data Protection	View Protection of Data at Rest [Incomplete]		
	View Incident Response [Incomplete]	Not Started	
Continuity Planning	View General [Incomplete]	Not Started	

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

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.

Additional Help				
Module	Sections		Module Status	Actions
Owner and Custodian Responsibilities	View	Resource Identification and Categorization [Complete]	Score: 100% Date Scored: 10-01-2013 11:37 AM	Your Next Steps
	View	Owner Responsibilities [Complete]		Assign All Signatories
	View	Custodian Responsibilities [Complete]		Other Actions
	View	Unit Responsibilities [Complete]		View/Edit Details View/Edit Signatories Answer Assessment Questions View/Edit Remediations Print Assessment Delete Assessment
Identity and Access Management	View	Identity and Authentication [Complete]	Score: 100% Date Scored: 10-01-2013 11:33 AM	
	View	Access Control [Complete]		
	View	Account Management [Complete]		
	View	Audit and Accountability [Complete]		
Platform Management	View	Systems Acquisition and Development [Complete]	Score: 100% Date Scored: 10-01-2013 11:37 AM	
Data Protection	View	Protection of Data at Rest [Complete]	Score: 100% Date Scored: 10-01-2013 11:37 AM	
	View	Incident Response [Complete]		

[Contact Us](#) • [Texas A&M University](#) • [Texas A&M Information Technology](#) • [Networking & Information Security](#) • [Site Policies](#) • [Webmaster](#)

Step 5: Print Report

Print the assessment by selecting the “Print Assessment” button on the Assessment Methodology page.

Additional Help				
Module	Sections		Module Status	Actions
Owner and Custodian Responsibilities	View	Custodian Responsibilities [Complete]	Score: 100% Date Scored: 10-01-2013 11:37 AM	Other Actions
	View	Unit Responsibilities [Complete]		View/Edit Details View/Edit Signatories Answer Assessment Questions View/Edit Remediations Print Assessment Delete Assessment
	View	Identity and Authentication [Complete]		
	View	Access Control [Complete]		
Identity and Access Management	View	Account Management [Complete]		
	View	Audit and Accountability [Complete]		
	View	Systems Acquisition and Development [Complete]		
	View	Protection of Data at Rest [Complete]		

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.